P23974.P04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Takafumi UENO

Serial No. : Not Yet Assigned

Filed : Concurrently Herewith

For : TRANMISSION APPARATUS AND RECEIVING APPARATUS

CLAIM OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Applicant hereby claims the right of priority granted pursuant to 35 U.S.C. 119 based upon Japanese Application No. 2002-210727, filed July 19, 2002. As required by 37 C.F.R. 1.55, a certified copy of the Japanese application is being submitted herewith.

Respectfully submitted,
Takafumi UENO

Bruce H. Bernstein
Reg. No. 29,027

Reg No 33,329

July 16, 2003
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　７月１９日

出願番号
Application Number: 特願２００２－２１０７２７

[ST.10/C]: [ＪＰ２００２－２１０７２７]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　６月１６日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４６８９５

【書類名】　特許願
【整理番号】　2054041179
【提出日】　平成14年 7月19日
【あて先】　特許庁長官殿
【国際特許分類】　H04K 1/00
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　上野　孝文
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100097445
【弁理士】
【氏名又は名称】　岩橋　文雄
【選任した代理人】
【識別番号】　100103355
【弁理士】
【氏名又は名称】　坂口　智康
【選任した代理人】
【識別番号】　100109667
【弁理士】
【氏名又は名称】　内藤　浩樹
【手数料の表示】
【予納台帳番号】　011305
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

出証特２００３－３０４６８９５

【書類名】　明細書

【発明の名称】　送信装置、及び受信装置

【特許請求の範囲】

【請求項１】　データを暗号化して第１の暗号化データを生成する暗号化手段と、

第１の暗号化データと第１の暗号化データのプログラム番号との対応を示すテーブルを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、

第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、

第１の暗号化データに付随する権利情報を生成する権利情報生成手段と、

第１の暗号化データと前記プログラム仕様情報と前記ツールリストと前記制御グラフと前記権利情報とを多重化する多重化手段とを有する送信装置。

【請求項２】　データを暗号化して第１の暗号化データを生成する暗号化手段と、

第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、

第１の暗号化データに付随する権利情報を生成する権利情報生成手段と、

第１の暗号化データと第１の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、

第１の暗号化データと前記プログラム仕様情報とを多重化する多重化手段とを有する送信装置。

【請求項３】　データを暗号化して第１の暗号化データを生成する暗号化手段と、

第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリ

出証特２００３－３０４６８９５

ストを生成するツールリスト生成手段と、

前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、

第１の暗号化データと第１の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、

前記データに付随する権利情報を生成する権利情報生成手段と、

前記権利情報を出力する権利情報送信手段と、

第１の暗号化データと前記プログラム仕様情報とを多重化して出力する多重化手段とを有する送信装置。

【請求項４】　前記権利情報と前記データとの対応付けを行う前記権利情報送信手段を有する請求項３に記載の送信装置。

【請求項５】　前記権利情報と前記データとの対応付けを行う前記プログラム仕様情報生成手段を有する請求項３に記載の送信装置。

【請求項６】　暗号を復号する復号ツールを多重化する前記多重化手段を有する請求項１乃至請求項５いずれかに記載の送信装置。

【請求項７】　暗号を復号するための鍵情報を多重化する前記多重化手段を有する請求項１乃至請求項６いずれかに記載の送信装置。

【請求項８】　第１の暗号化データを含む多重化信号を少なくとも第１の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、

前記多重化信号から第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを分離するツールリスト分離手段と、

前記多重化信号から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、

前記多重化信号から第１の暗号化データに付随する権利情報を分離する権利情報手段と、

前記ツールリストから取得したツールＩＤに従ってツールを入手し、前記制御グラフに従って前記ツールを組み込む第１の制御手段と、

前記権利情報に従って第１の暗号化データを処理する第１の権利管理手段とを

有する受信装置。

【請求項９】　第１の暗号化データを含む多重化信号を少なくとも第１の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、

前記プログラム仕様情報から第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを分離するツールリスト分離手段と、

前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、

前記プログラム仕様情報から第１の暗号化データに付随する権利情報を分離する権利情報手段と、

前記ツールリストから取得したツールＩＤを有するツールを前記制御グラフに従って組み込む第１の制御手段と、

前記権利情報に従って第１の暗号化データを処理する第１の権利管理手段とを有する受信装置。

【請求項１０】　第１の暗号化データを含む多重化信号を少なくとも第１の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、

前記プログラム仕様情報から第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを分離するツールリスト分離手段と、

前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、

前記ツールリストから取得したツールＩＤを有するツールを前記制御グラフに従って組み込む第１の制御手段と、

第１の暗号化データに付随する権利情報を受信する権利情報受信手段と、

前記権利情報に従って第１の暗号化データを処理する第１の権利管理手段とを有する受信装置。

【請求項１１】　受信した第１の暗号化データを一時的に記憶する一時記憶手段と、

前記一時記憶手段に記憶された第１の暗号化データを読み取る読み取り手段を有する請求項８乃至請求項１０いずれかに記載の受信装置。

【請求項１２】　前記権利情報に記述された再生許諾が満了した後に第１の暗

号化データを前記一時記憶手段から消去するファイル管理手段を有する請求項１１に記載の受信装置。

【請求項１３】　第１の暗号化データの処理状態を示す状態情報を送信する前記権利管理手段を有する請求項８乃至請求項１２いずれかに記載の受信装置。

【請求項１４】　前記権利情報を第１の権利情報と第２の権利情報とに分割する権利管理手段と、

前記多重化信号のうちの前記権利情報を第２の権利情報に書き換えて修正多重化信号を出力する多重化修正手段と、

第２の受信装置からの要求信号に応じて前記修正多重化信号を第２の受信装置に出力する請求項８乃至請求項１３に記載の受信装置。

【請求項１５】　前記権利情報を第１の権利情報と第２の権利情報とに分割する権利管理手段と、

第２の受信装置からの要求信号に応じて第２の権利情報と前記多重化信号を第２の受信装置に出力する請求項８乃至請求項１３いずれかに記載の受信装置。

【請求項１６】　前記権利管理手段は第２の受信装置における第１の暗号化データの処理状態を示すデータを受信し自身と第２の受信装置の処理状態を示す状態情報を送信することを特徴とする請求項８乃至請求項１５いずれかに記載の受信装置。

【請求項１７】　第１の暗号化データを第２の暗号化データに変換する変換手段と、

第２の暗号化データを第２の権利情報とともに再多重化する再多重化手段を有する請求項８乃至請求項１６いずれかに記載の受信装置。

【請求項１８】　第１の権利情報によって第１の暗号化データを処理する請求項８乃至請求項１７いずれかに記載の受信装置。

【請求項１９】　第１の暗号化データを第２の受信手段に転送後、前記第１の暗号化データを前記一次記憶手段から消去するファイル管理手段を有する請求項１４乃至請求項１８いずれかに記載の受信装置。

【請求項２０】　前記多重化信号からビデオデータを抽出し復号するビデオ復号手段を有する請求項８乃至請求項１９いずれかに記載の受信装置。

【請求項２１】　前記多重化信号からオーディオデータを抽出し復号するオーディオ復号手段を有する請求項８乃至請求項１９いずれかに記載の受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像圧縮された動画と番組情報を多重化したディジタル放送信号を送信する装置、及び受信する装置に関するものである。

【０００２】

【従来の技術】

図１５は、従来例における送信装置と受信装置を示すブロック図である。図１５において、４９は入力ディジタルビデオ信号、５０は入力ディジタルオーディオ信号、５６はＭＰＥＧ－２ビデオ（ＩＳＯ／ＩＥＣ１３８１８－２）に準拠したビデオ符号化手段、５７はＭＰＥＧ－２オーディオ（ＩＳＯ／ＩＥＣ１３８１８－３）に準拠したオーディオ符号化手段、６４はオーディオビットストリーム、７６はビデオビットストリーム、５９はプログラム仕様情報生成手段、５００はプログラム仕様情報、６６はＭＰＥＧ－２システムズ（ＩＳＯ／ＩＥＣ－１３８１８－１）に準拠した多重化手段、５０１は多重化ビットストリーム、１０７は多重化分離手段、１１０はビデオビットストリーム、１２６はオーディオビットストリーム、１１２はビデオ復号手段、１１３はオーディオ復号手段、１１１はディジタルビデオ信号、１１４はディジタルオーディオ信号、５０３は受信装置である。

【０００３】

図１５にて、従来の送信装置５０２では、入力ディジタルビデオ信号４９は、ビデオ符号化手段５６によってＭＰＥＧ－２ビデオに準拠して圧縮符号化されビデオビットストリーム７６として出力される。入力ディジタルオーディオ信号５０は、オーディオ符号化手段５７によって圧縮符号化されオーディオビットストリーム６４として出力される。プログラム仕様情報生成手段５９は、ビデオビットストリーム７６、オーディオビットストリーム６４とプログラム番号との関係を示すプログラム仕様情報５００を生成する。多重化手段６６はビデオビットス

トリーム７６、オーディオビットストリーム６４、プログラム仕様情報５００を多重化して多重化ビットストリーム５０１を生成する。

【０００４】

従来の受信装置５０３では、多重化情報５００は多重化分離手段１０７によってビデオビットストリーム１１０、オーディオビットストリーム１２６とに分離される。ビデオビットストリーム１１０はビデオ復号手段１１１によって伸長されディジタルビデオ信号１１２として出力される。オーディオビットストリーム１２６はオーディオ復号手段１１３によって伸長されディジタルオーディオ信号１１４として出力される。

【０００５】

【発明が解決しようとする課題】

しかしながら、上記において、ビデオビットストリーム等の暗号化は行われておらず、不正な受信装置によって容易に盗むことが可能である。また、仮に暗号化を施しても暗号化手法自体を不正に解読されることに対する対処もなされていない。すなわち、送信装置が送信したデータの不正な受信を防ぐ手段がないという課題がある。

【０００６】

本発明は、上記課題を考慮し、送信装置が送信したデータを受信装置が安全に受信する保護手段を提供することを目的とするものである。

【０００７】

【課題を解決するための手段】

上述した課題を解決するために、第１の発明（請求項１に対応）は、データを暗号化して第１の暗号化データを生成する暗号化手段と、第１の暗号化データと第１の暗号化データのプログラム番号との対応を示すテーブルを含むプログラム仕様情報を生成するプログラム仕様情報手段と、第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第１の暗号化データに付随する権利情報を生成する権利情報生成手段と、第１の暗号化データと前記プログラム仕様情報と前記ツール

リストと前記制御グラフと前記権利情報とを多重化する多重化手段とを有する送信装置である。

【０００８】

また、第２の発明（請求項２に対応）は、データを暗号化して第１の暗号化データを生成する暗号化手段と、第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第１の暗号化データに付随する権利情報を生成する権利情報生成手段と、第１の暗号化データと第１の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、第１の暗号化データと前記プログラム仕様情報とを多重化する多重化手段とを有する送信装置である。

【０００９】

また、第３の発明（請求項３に対応）は、データを暗号化して第１の暗号化データを生成する暗号化手段と、第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを生成するツールリスト生成手段と、前記復号ツールの受信装置での組み込み位置を示す制御グラフを生成する制御グラフ生成手段と、第１の暗号化データと第１の暗号化データのプログラム番号との対応を示すテーブルと前記ツールリストと前記制御グラフと前記権利情報とを含むプログラム仕様情報を生成するプログラム仕様情報生成手段と、前記データに付随する権利情報を生成する権利情報生成手段と、前記権利情報を出力する権利情報送信手段と、第１の暗号化データと前記プログラム仕様情報とを多重化して出力する多重化手段とを有する送信装置である。

【００１０】

また、第４の発明（請求項４に対応）は、前記権利情報と前記データとの対応付けを行う前記権利情報送信手段を有する第３の発明に記載の送信装置。

【００１１】

また、第５の発明（請求項５に対応）は、前記権利情報と前記データとの対応付けを行う前記プログラム仕様情報生成手段を有する第３の発明に記載の送信装

置である。

【００１２】

また、第６の発明（請求項６に対応）は、暗号を復号する復号ツールを多重化する前記多重化手段を有する第１の発明乃至第５の発明いずれかに記載の送信装置。

【００１３】

また、第７の発明（請求項７に対応）は、暗号を復号するための鍵情報を多重化する前記多重化手段を有する第１の発明乃至第６の発明いずれかに記載の送信装置。

【００１４】

また、第８の発明（請求項８に対応）は、第１の暗号化データを含む多重化信号を少なくとも第１の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、前記多重化信号から第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを分離するツールリスト分離手段と、前記多重化信号から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、前記多重化信号から第１の暗号化データに付随する権利情報を分離する権利情報手段と、前記ツールリストから取得したツールＩＤに従ってツールを入手し、前記制御グラフに従って前記ツールを組み込む第１の制御手段と、前記権利情報に従って第１の暗号化データを処理する第１の権利管理手段とを有する受信装置である。

【００１５】

また、第９の発明（請求項９に対応）は、第１の暗号化データを含む多重化信号を少なくとも第１の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、前記プログラム仕様情報から第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを分離するツールリスト分離手段と、前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、前記プログラム仕様情報から第１の暗号化データに付随する権利情報を分離する権利情報手段と、前記ツールリストから取得したツールＩＤを有するツールを前記制御グラフに従って組み込む第

１の制御手段と、前記権利情報に従って第１の暗号化データを処理する第１の権利管理手段とを有する受信装置である。

【００１６】

また、第１０の発明（請求項１０に対応）は、第１の暗号化データを含む多重化信号を少なくとも第１の暗号化データとプログラム仕様情報とに分離する多重化分離手段と、前記プログラム仕様情報から第１の暗号化データを復号する復号ツールを示すツールＩＤを有するツールリストを分離するツールリスト分離手段と、前記プログラム仕様情報から前記復号ツールの受信装置での組み込み位置を示す制御グラフを分離する制御グラフ分離手段と、前記ツールリストから取得したツールＩＤを有するツールを前記制御グラフに従って組み込む第１の制御手段と、第１の暗号化データに付随する権利情報を受信する権利情報受信手段と、前記権利情報に従って第１の暗号化データを処理する第１の権利管理手段とを有する受信装置である。

【００１７】

また、第１１の発明（請求項１１に対応）は、受信した第１の暗号化データを一時的に記憶する一時記憶手段と、前記一時記憶手段に記憶された第１の暗号化データを読み取る読み取り手段を有する第８の発明乃至第１０の発明いずれかに記載の受信装置である。

【００１８】

また、第１２の発明（請求項１２に対応）は、前記権利情報に記述された再生許諾が満了した後に第１の暗号化データを前記一時記憶手段から消去するファイル管理手段を有する第１１の発明に記載の受信装置である。

【００１９】

また、第１３の発明（請求項１３に対応）は、第１の暗号化データの処理状態を示す状態情報を送信する前記権利管理手段を有する第８の発明乃至第１２の発明いずれかに記載の受信装置である。

【００２０】

また、第１４の発明（請求項１４に対応）は、前記権利情報を第１の権利情報と第２の権利情報とに分割する権利管理手段と、前記多重化信号のうちの前記権

利情報を第２の権利情報に書き換えて修正多重化信号を出力する多重化修正手段と、第２の受信装置からの要求信号に応じて前記修正多重化信号を第２の受信装置に出力する第８の発明乃至第１２の発明いずれかに記載の受信装置である。

【００２１】

また、第１５の発明（請求項１５に対応）は、前記権利情報を第１の権利情報と第２の権利情報とに分割する権利管理手段と、第２の受信装置からの要求信号に応じて第２の権利情報と前記多重化信号を第２の受信装置に出力する第８の発明乃至第１３の発明いずれかに記載の受信装置である。

【００２２】

また、第１６の発明（請求項１６に対応）は、前記権利管理手段は第２の受信装置における第１の暗号化データの処理状態を示すデータを受信し自身と第２の受信装置の処理状態を示す状態情報を送信することを特徴とする第８の発明乃至第１５の発明いずれかに記載の受信装置である。

【００２３】

また、第１７の発明（請求項１７に対応）は、第１の暗号化データを第２の暗号化データに変換する変換手段と、第２の暗号化データを第２の権利情報とともに再多重化する再多重化手段を有する第８の発明乃至第１６の発明いずれかに記載の受信装置である。

【００２４】

また、第１８の発明（請求項１８に対応）は、第１の権利情報によって第１の暗号化データを処理する第８の発明乃至第１７の発明いずれかに記載の受信装置である。

【００２５】

また、第１９の発明（請求項１９に対応）は、第１の暗号化データを第２の受信手段に転送後、前記第１の暗号化データを前記一次記憶手段から消去するファイル管理手段を有する第１４の発明乃至第１８の発明いずれかに記載の受信装置である。

【００２６】

また、第２０の発明（請求項２０に対応）は、前記多重化信号からビデオデー

タを抽出し復号するビデオ復号手段を有する第８の発明乃至第１９の発明いずれかに記載の受信装置である。

【００２７】

また、第２１の発明（請求項２１に対応）は、前記多重化信号からオーディオデータを抽出し復号するオーディオ復号手段を有する第８の発明乃至第１９の発明いずれかに記載の受信装置である。

【００２８】

【発明の実施の形態】

以下、本発明の実施の形態について、図１～図１４を用いて説明する。

【００２９】

（第１の実施の形態）

図１は、本発明の第１の実施の形態における送信装置を示すブロック図である。図１において、４９、５０、５６、５７、５９、６４、７６は図１５に示す従来例の構成と同様であり、５１は権利情報生成手段、５２はツールリスト生成手段、５３は制御グラフ生成手段、５８はストリーム情報生成手段、６０はＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）に準拠した鍵長１２８ビットの暗号化を行う暗号化手段、６１はプログラム仕様情報生成手段、６２はＭＰＥＧ－２システムズ（ＩＳＯ／ＩＥＣ－１３８１８－１）に準拠した多重化手段、６３は暗号化ビデオビットストリーム、６５はプログラム仕様情報、６６は多重化ビットストリーム、６７は権利情報生成手段５１によって生成される権利情報、６８はツールリスト生成手段５２によって生成されるツールリスト、６９は制御グラフ生成手段５３によって生成される制御グラフ、７２はストリーム情報、７３は第１の送信装置、７４は状態情報、７５は送信制御手段、８１は権利制御情報、８２はツール制御情報、８３はグラフ制御情報、１１５は復号ツールである。

【００３０】

図１にて、入力ディジタルビデオ信号４９は、ビデオ符号化手段５６によってＭＰＥＧ－２準拠のビデオビットストリーム７６に圧縮符号化され、第１の暗号化手段６０によって暗号化され暗号化ビデオビットストリーム６３として出力さ

れる。入力ディジタルオーディオ信号５０は、オーディオ符号化手段５７によって圧縮符号化されオーディオビットストリーム６４として出力される。

【００３１】

表１に状態情報７４を示す。表１に示す各値は８ビットで表され、ビット７～ビット０で表されるものとする。送信デバイスＩＤをもつ送信装置から受信デバイスＩＤをもつ受信装置との間で状態情報及び内容を交信する。状態情報は表１に示す各値をもつものとし、内容の項にその内容を記入する。

【００３２】

【表１】

状態情報	
ツール要求	0X10000000
コンテント要求	0X01000000
コピー情報	0X00100000
再生回数	0X00010000
編集	0X00001000

【００３３】

権利情報生成手段５１は、コンテント毎にコンテントの利用条件を示す権利情報を作成してプログラム仕様情報生成手段５９に供給する。表２の値は、状態情報が各々コピー情報、再生回数、編集である場合に対応して表１の内容のところに記入される。ここでプログラムとはコンテントにプログラム仕様情報を付加した番組を示すことにする。

【００３４】

【表２】

コピー情報	１回	0X00000000
	禁止	0X00000001
再生回数		1Xnnnnnnnn
編集	許可	0X00000010
	禁止	0X00000011

【００３５】

本発明の第１の実施の形態では、Ａ、Ｂの２種類のプログラムを含むものとする。プログラムＡは表３に示す値で送るものとする。すなわち、コピー１回、再生回数１回、編集禁止である。

【００３６】

【表３】

コンテント		プログラムA
コピー	１回	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【００３７】

プログラムＢは表４に示す値で送るものとする。すなわち、コピー１回、再生回数３回、編集禁止である。

【００３８】

【表４】

コンテント		プログラムB
コピー	１回	0X00000000
再生回数		1X00000003
編集	禁止	0X00000011

【００３９】

送信装置７３は、ＡＥＳ復号を実行するツールＩＤ（０Ｘ００Ａ）を有する復号ツール１１５が存在することを認識しているものとする。ツールリスト生成手段５２は、受信装置側等で必要となるツールの一覧表を生成してプログラム仕様情報生成手段５９に供給する。ツールリスト生成手段５２では、ＭＰＥＧ－２ビデオビットストリームを受信し再生するために復号ツール１１５が必要であることを示し上記ツールＩＤ（０Ｘ００Ａ）を有するツールリストを生成する。

【００４０】

制御グラフ６９の構成の一部を図２に示す。プログラムＡは暗号化ビデオビットストリーム６３とオーディオビットストリーム６４を含み、暗号化ビデオビットストリーム６３に対応するツールＩＤ、ツールの組み込み位置を示す制御ポイントを有している。プログラムＢも同様である。

【００４１】

制御グラフ生成手段５３は、ＡＥＳ復号を実行するツールＩＤ（０Ｘ００Ａ）を有するツールの組み込み位置が受信装置のビデオ復号手段の直前であることを示す制御グラフ６９を生成してプログラム仕様情報生成手段６１に出力する。

【００４２】

プログラム仕様情報生成手段６１は、暗号化ビデオビットストリーム６３とオーディオビットストリーム６４とプログラムのプログラム番号との関係を示す関係表とともに権利情報６７、ツールリスト６８、制御グラフ６９を含むプログラム仕様情報６５を生成する。

【００４３】

ストリーム情報生成手段５８は、暗号化手段６０で用いられている暗号を解く為の鍵情報などが入ったストリーム情報７２を作成する。

【００４４】

多重化手段６２は暗号化ビデオビットストリーム６３、オーディオビットストリーム６４、プログラム仕様情報６５、ストリーム情報７２、復号ツール１１５をＭＰＥＧ－２システムズに準拠して多重化し、多重化ビットストリーム６６を生成する。

【００４５】

また、送信制御手段７５は状態情報７４を他の機器から受け取ることによって、本発明の第１の実施の形態の送信装置が許諾した権利情報６７が他の機器でどのように処理されたかを知ることができる。ここでは、表４に示すプログラムＢの権利情報が表５に示す状態情報７４として本発明の送信装置で受信されたとすると、１回コピーされ、２回再生されたことがわかる。

【００４６】

【表５】

コンテント		プログラムB
コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【００４７】

以上のように、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるのでツールを更新することが可能であり、常に最新の保護方式を提供するとともに、多重化情報のプログラ

ム仕様情報の一部として処理することができるという利便性を送信装置を提供することができる。

【００４８】

また、本発明の第１の実施の形態では、権利情報６７、ツールリスト６８、制御グラフ６９をプログラム仕様情報生成手段５９に加えているがプログラム仕様情報生成手段５９を経ずに直接多重化情報生成手段６２に加えてもよい。この場合には、権利情報６７、ツールリスト６８、制御グラフ６９はプログラム仕様情報に含まれないのでより簡便な送信装置を提供することができる。

【００４９】

（第２の実施の形態）

図３は、本発明の第２の実施の形態における送信装置を示すブロック図である。図３において、４９、５０、５６、５７、６４、７６は図１５に示す従来例の構成と同様であり、５１～５３、５８、６０～６３、６５～６９、７２、７４、７５、８１～８３は図１に示す本発明の第１の実施の形態と同様であり、８４は権利情報送信手段、８５は送信権利情報、８６は第２の送信装置である。

【００５０】

図３にて、入力ディジタルビデオ信号４９は、ビデオ符号化手段５６によってＭＰＥＧ－２準拠のビデオビットストリーム７６に圧縮符号化され、暗号化手段６０によって暗号化され暗号化ビデオビットストリーム６３として出力される。入力ディジタルオーディオ信号５０は、オーディオ符号化手段５７によって圧縮符号化されオーディオビットストリーム６４として出力される。

【００５１】

状態情報７４は表１と同様であり、権利情報生成手段５１は、コンテント毎にコンテントの利用条件を示す権利情報６７を作成して権利情報送信手段８４に供給する。表６に権利情報６７を示す。

【００５２】

【表６】

コピー	１回	0X00000000
	禁止	0X00000001
再生回数		1Xnnnnnnnn
編集	許可	0X00000010
	禁止	0X00000011

【００５３】

本発明の第２の実施の形態では、プログラムＡ，プログラムＢの２種類のコンテンツを含むものとする。プログラムＡは表７に示す値で送るものとする。すなわち、コピー１回、再生回数１回、編集禁止である。表７で権利情報はプログラムＡとの対応付けが行われている。

【００５４】

【表７】

コンテント		プログラムA
コピー	１回	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【００５５】

プログラムＢは表８に示す値で送るものとする。すなわち、コピー１回、再生回数３回、編集禁止である。表８で権利情報はプログラムＢとの対応付けが行われている。

【００５６】

【表８】

コンテント		プログラムB
コピー	１回	0X00000000
再生回数		1X00000003
編集	禁止	0X00000011

【００５７】

送信装置８６は、ＡＥＳ復号を実行するツールＩＤ（０Ｘ００Ａ）を有する復号ツール１１５があることを認識しているものとする。ツールリスト生成手段５２は、受信装置側等で必要となるツールの一覧表を生成してプログラム仕様情報生成手段６１に供給する。すなわち、ＭＰＥＧ－２ビデオビットストリームを受

信し再生するために復号ツール１１５が必要であることを示し上記ツールＩＤ（０Ｘ００Ａ）を有するツールリスト６８を生成する。

【００５８】

制御グラフの構成は図２と同様である。プログラムＡは第１の暗号化ビットストリーム６３とオーディオビットストリーム６４を含み、第１の暗号化ビットストリーム６３に対応するツールＩＤ、ツールが組み込まれる組み込み位置を示す制御ポイントを有している。プログラムＢも同様である。

【００５９】

制御グラフ生成手段５３は、上記ＡＥＳ復号を実行するツールＩＤ（０Ｘ００Ａ）を有するツールの組み込み位置が受信装置のビデオ復号手段の手前であることを示す制御グラフ６９を生成してプログラム仕様情報生成手段６１に出力する。

【００６０】

プログラム仕様情報生成手段６１は、暗号化ビデオビットストリーム６３とオーディオビットストリーム６４とプログラムのプログラム番号との関係を示す関係表とともにツールリスト６８、制御グラフ６９と復号ツール１１５を含むプログラム仕様情報６５を生成する。

【００６１】

ストリーム情報生成手段５８は、暗号化手段６０で用いられている暗号を解く為の鍵情報などが入ったストリーム情報７２を作成する。

【００６２】

多重化手段６２は暗号化ビデオビットストリーム６３、オーディオビットストリーム６４、プログラム仕様情報６５、ストリーム情報７２を上記ＭＰＥＧ－２システムズに準拠して多重化し、多重化ビットストリーム６６を生成する。

【００６３】

権利情報送信手段８４は、権利情報６７とプログラムとの対応付けを行う。ここでは、プログラム仕様情報生成手段との通信によって暗号化ビデオビットストリーム６３とオーディオビットストリーム６４とプログラムのプログラム番号との関係を示す関係表が得られるのでプログラムとの対応付けを行うことができ、

その後、ファイル化して送信権利情報８５として送信する。権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利点がある。

【００６４】

また、送信制御手段７５は状態情報７４を他の機器から受け取ることによって、本発明の第１の実施の形態の送信装置が許諾した権利情報６７が他の機器でどのように処理されたかを知ることができる。ここでは、表８に示す権利情報が表９に示す権利情報として本発明の送信装置で受信されたとすると、１回コピーされ、２回再生されたことがわかる。

【００６５】

【表９】

コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【００６６】

以上のように、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるのでツールを更新することが可能であり、常に最新の保護方式を提供するとともに、権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利便性を送信装置を提供することができる。

【００６７】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るとともに権利情報と多重化情報との対応付けも行うことができるので、複数の多重化情報と権利情報が混在する場合にも各々区別することができるという利便性を有する送信装置を提供することができる。

【００６８】

（第３の実施の形態）

図４は、本発明の第３の実施の形態における受信装置を示すブロック図である。図４において、１１１～１１４は図１５に示す従来例の構成と同様であり、１００は第１の受信装置、１０１は入力されるＭＰＥＧ－２システムズ準拠の第１の多重化ビットストリーム、１０２はハードディスク記憶手段、１０３はハードディスク記憶手段１０２から読み出された読み出し多重化ビットストリーム、１０８は組み込み手段、１１０はビデオビットストリーム、１１５はＡＥＳ暗号を復号する復号ツール、１２０は第１の制御手段、１２１は第１の権利管理手段、１２３はファイル管理情報、１２４はファイル管理手段、１２５はハードディスク１０２に対する指令、９０はストリーム情報及び復号ツール１１５を含む読み出し情報、９１はプログラム仕様情報分離手段、９２はプログラム仕様情報、９３は制御グラフ分離手段、９４は制御グラフ情報、９５はツールリスト分離手段、９６はツールリスト、９７は権利情報分離手段、９８は権利情報、１３２は第１の返信情報、１３７は第１の要求情報である。また、第１の受信装置１００は第１の送信装置７３に接続されているものとする。

【００６９】

図４にて、入力されるＭＰＥＧ－２システムズ準拠の第１の多重化ビットストリーム１０１はハードディスク１０２に一時的に記憶された後に読み出され読み出し多重化ビットストリーム１０３として多重化分離手段１０４に加えられる。多重化分離手段１０４は読み出し多重化ビットストリーム１０３を第１の暗号化ビデオビットストリーム１０５とオーディオビットストリーム１０６とプログラム仕様情報９２とストリーム情報９０とに分離する。

【００７０】

ここで、プログラム仕様情報９２は、第１の暗号化ビデオビットストリーム１０５、オーディオビットストリーム６４とプログラムのプログラム番号との関係を示す情報とともに、上記プログラムに付随する権利情報９８とＡＥＳ復号を実行するツールＩＤ（０Ｘ００Ａ）を有するツールリスト９６と上記復号ツールの組み込み位置が受信装置１００の多重化分離手段１０４とビデオ復号手段１１２との間であることを示す制御グラフ９４を含むものとする。また、読み出し情報

９０には、第１の暗号化ビデオビットストリーム１０５の暗号を解く為の鍵情報などが入っているものとする。

【００７１】

読み出し情報９０は多重化分離手段１０４で分離されて第１の制御手段１２０に加えられる。プログラム仕様情報９２はプログラム仕様情報分離手段９１に加えられる。制御グラフ分離手段９３はプログラム仕様情報分離手段９１から制御グラフ９４を抽出して第１の制御手段１２０に供給する。ツールリスト分離手段９５はプログラム仕様情報分離手段９１からツールリスト９６を抽出して第１の制御手段１２０に供給する。権利情報分離手段９７はプログラム仕様情報分離手段９１から権利情報９８を抽出して第１の権利管理手段１２１に供給する。

【００７２】

第１の制御手段１２０は表１０に示す第１の要求情報１３７を送信する。ここではツール要求とコンテンツすなわちプログラム要求を送っている。

【００７３】

【表１０】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【００７４】

第１の制御手段１２０は、ツールリスト９６から復号に必要なツールが復号ツール１１５であることを求め、制御グラフ９４から復号ツール１１５を適用する制御ポイントすなわち組み込み位置が１０８であることを求めるとともに読み出し情報９０からスクランブルを解くための鍵情報を抽出する。

【００７５】

第１の制御手段１２０は、復号ツール１１５の組み込み位置が受信装置１００の多重化分離手段１０４とビデオ復号手段１１２との間であることを示す制御グラフ９４に従って、組み込み手段１０８に復号ツール１１５とストリーム情報１１８から抽出された上記鍵情報が組み込む指示を出し、組み込み手段１０８は復号ツール１１５と上記鍵情報を組み込む。第１の暗号化ビデオビットストリーム１０５は組み込み手段１０８によって暗号を解読されてビデオビットストリーム

１１０として出力される。

【００７６】

ビデオビットストリーム１１０はビデオ復号手段１１１によって伸長されディジタルビデオ信号１１２として出力される。オーディオビットストリーム１０６はオーディオ復号手段１１３によって伸長されディジタルオーディオ信号１１４として出力される。

【００７７】

第１の権利管理手段１２１は権利情報９８を取得し、ファイル管理情報１２３をファイル管理手段１２４に出力する。ファイル管理手段１２４は、プログラムＡの場合、表４に与えられた再生回数は１回であるため、１回再生するとファイル管理手段１２４は、指令１２５をハードディスク１０２に出してハードディスク１０２上に記憶されたプログラムＡを消去する。

【００７８】

また、第１の権利管理手段１２１は第２の返信情報１３２として表１１に示す情報を返信する。ここでは第１の受信装置１００で１回再生されている。

【００７９】

【表１１】

コピー	許可	0X00000000
第１の受信装置での再生回数		0X00000001

【００８０】

（第４の実施の形態）

図５は、本発明の第４の実施の形態における受信装置を示すブロック図である。本発明の第４の実施の形態は受信装置がネットワークを通じて接続されている別の受信装置にツールをダウンロード、ディジタルデータを転送、サーバに消費情報を転送することができる。図５において、１１１～１１４は図１５に示す従来例の構成と同様であり、９０～９８、１０１～１０６、１０８、１１０、１１５、１２３～１２５、１３２は本発明の第３の実施の形態と同様であり、１３０は第２の受信装置、１３３は第２の権利情報、１３６は第２の返信情報、１３８は第２の権利管理手段、１３９は第２の制御手段、１４０は第２の要求情報、１

４１は第１の制御情報、１４２は多重化修正手段、１４３はＭＰＥＧ－２システムズ準拠の第２の多重化ビットストリーム、１４４は第１０の受信装置である。図６は、第２の権利管理手段１３８の処理の概略を示す図である。図７は、第１の多重化ビットストリーム１０３と第２の多重化ビットストリーム１４３の概略の構成を示す図であり、１４６は暗号化ビデオビットストリーム６３とオーディオビットストリーム６４とプログラムＡのプログラム番号との関係を示す関係表である。また、図５において、第２の受信装置１３０は送信装置７３に接続されているものとし、第２の受信装置１３０に接続されている第１０の受信装置１４４は図４に示す第１の受信装置と等価な機能を有するものとする。

【００８１】

図５にて、読み出し情報９０は多重化分離手段１０４で分離されて第２の制御手段１３９に加えられる。第２の制御手段１３９は、第２の権利管理手段１３８に権利許諾の情報を出すとともに多重化修正手段１４２に多重化ビットストリーム修正を含む第１の制御情報１４１を送る。

【００８２】

第２の制御手段１３９は第１０の受信装置１４４から表１２に示す第２の要求情報１４０を受け取る。表１２は第１０の受信装置１４４が第２の受信装置１３０に対してツールとコンテントを要求していることを示している。

【００８３】

【表１２】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【００８４】

図６は第２の権利管理手段１３８の動作の一部を示している。ステップ１において、第２の制御手段１３９を経由して第２の要求情報１４０を受信する、ステップ２で権利情報９８を受信し、ステップ３で権利情報９８を第２の受信装置１３０で使用する第１の権利情報と第１０の受信装置１４４で使用する第２の権利情報１３３に分割する。ステップ４で第１の権利情報を出力し、ステップ５で第１の権利情報に基づいてファイル管理情報１２３をファイル管理手段１２４に出

力し、ステップ６で第２の権利情報１３３を出力する。

【００８５】

第２の受信装置１３０で表４に示す権利情報を有するプログラムＢを１回再生するとともに第１の受信装置に転送するものとすると、第１の権利情報を表１３、第２の権利情報を表１４のように表わすことができる。第１０の受信装置１４４に転送する第２の権利情報を示す表１４では第２の受信装置１３０で１回再生するので再生回数を１回減じている。

【００８６】

【表１３】

コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【００８７】

【表１４】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【００８８】

第２の権利管理手段１３８は表１４に示す第２の権利情報１３３を多重化修正手段１４２に送る。多重化修正手段１４２は第１の多重化ビットストリーム１０３に第２の権利情報１３３をもとに修正を加える。すなわち、第１の多重化ビットストリーム１０３の権利情報１２２を第２の権利情報１３３の内容に変更して第２の多重化ビットストリーム１４３を出力する。

【００８９】

図７は第１の多重化ビットストリームと第２の多重化ビットストリームの構成を示している。権利情報９８は第２の権利管理手段によって第２の権利情報１３３として多重化修正手段１４２に加えられ、第２の多重化ビットストリーム１４３では第２の権利情報が含まれる。

【００９０】

第２の制御手段１３９は、復号ツール１１５の組み込み位置が第２の受信装置１３０の多重化分離手段１０４とビデオ復号手段１１２との間であることを示す制御グラフ９４に従って、組み込み手段１０８に復号ツール１１５とストリーム情報１１８から抽出された上記鍵情報を組み込む指示を出し、組み込み手段１０８は復号ツール１１５と上記鍵情報を組み込む。第１の暗号化ビデオビットストリーム１０５は組み込み手段１０８によって暗号を解読されてビデオビットストリーム１１０として出力され、ビデオ復号手段１１２によって復号されてディジタルビデオ信号として出力される。

【００９１】

その他の動作は本発明の第３の実施の形態と同様である。これによって、第２の受信装置１３０は、受信した権利情報、ビットストリーム、ツール情報等をネットワーク上で接続された第１０の受信装置１４４に送ることが可能となる。

【００９２】

また、第２の権利管理手段１３８は、第１０の受信装置１４４から送られる第２の返信情報１３６をもとにして第１の返信情報１３２を出力する。この場合、第２の受信装置１３０及び第１０の受信装置１４４での再生回数は１回であるとすると、表１５のように構成される第１の返信情報を出力する。

【００９３】

【表１５】

第２の受信装置での再生回数		0X00000001
第１の受信装置での再生回数		0X00000001

【００９４】

これによって送信装置は、第２の受信装置１３０及び第２の受信装置１３０に接続された第１０の受信装置１４４での消費情報を得ることができる。

【００９５】

（第５の実施の形態）

図８は、本発明の第５の実施の形態における受信装置を示すブロック図である。本発明の第５の実施の形態は受信装置が受信した権利情報をダウンロード、ディジタルデータをネットワークに接続されている別の受信装置に転送するととも

にサーバに消費情報を転送することができる。図８において、１１１～１１４は図１５に示す従来例の構成と同様であり、９０～９８、１０１～１０６、１０８、１１０、１１５、１２３～１２５、１３２、１３７は図４に示す本発明の第３の実施の形態と同様であり、１３６、１４０は図５に示す本発明の第４の実施の形態と同様であり、１５０は第３の受信装置、１５３は第３の権利情報、１５４は第４の受信装置、１６０は第３の制御手段、１６１は第３の権利管理手段である。

【００９６】

図８にて、第３の制御手段１６０は第４の受信装置１５４から表１６に示す第２の要求情報１４０を受け取るものとする。表１６は第４の受信装置１５４が第３の受信装置１５０に対してツールとコンテントを要求していることを示している。第３の制御手段１６０は第３の権利管理手段１６１に権利許諾の情報を出す。

【００９７】

【表１６】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【００９８】

読み出し情報９０は多重化分離手段１０４で分離されて第３の制御手段１６０に加えられる。第３の権利管理手段１６１は、権利情報９８を第３の受信装置１５０で使用する第１の権利情報と第４の受信装置１５４で使用する第３の権利情報１５３とに分割し、第３の権利情報１５３を第４の受信装置１５４に送る。

【００９９】

ここでは第３の受信装置１５０で１回再生し、第４の受信装置１５４で１回再生するものとすると、第１の権利情報及び第３の権利情報１５３は各々表１７、表１８となる。表１８では第３の受信装置１５０で１回再生しているので再生回数を１回減じている。

【０１００】

【表１７】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【０１０１】

【表１８】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【０１０２】

その他の動作は本発明の第３の実施の形態と同様である。これによって、第３の受信装置１５０は、受信した権利情報、ビットストリーム、ツール情報等を第４の受信装置１５４に送ることが可能となる。

【０１０３】

（第６の実施の形態）

図９は、本発明の第６の実施の形態における受信装置を示すブロック図である。本発明の第６の実施の形態は第３の受信装置にホームネットワークを経由して接続された第４の受信装置に関するものである。図９において、１１１～１１４は図１５に示す従来例の構成と同様であり、９０～９８、１０１～１０６、１０８、１１０、１１５、１２３～１２５、１３７は図４に示す本発明の第３の実施の形態と同様であり、１３６は図５に示す本発明の第４の実施の形態と同様であり、１５４は第４の受信装置、２３１は第４の制御手段、２３２は第４の権利管理手段である。

【０１０４】

図９にて、読み出し情報９０は多重化分離手段１０４で分離されて第４の制御手段２３１に加えられる。第４の権利管理手段２３２は権利情報９８をもとにして、第４の受信装置１５４での消費状況とをもとに第２の返信情報１３６を生成する。第２の返信情報１３６は、ディジタルビデオ情報１１２及びディジタルオーディオ情報１１４を第４の受信装置で再生したことを示す消費情報として再生

回数を１回減じる。その結果、表１８のように与えられるプログラムＢの権利情報は表１９のように書き換えられる。

【０１０５】

【表１９】

コンテンツ	許可	プログラムB
コピー	禁止	0X00000001
再生回数		1X00000001
編集	禁止	0X00000011

【０１０６】

表１９のように書き換えられた第２の返信情報１３６は第４の権利管理手段２３２から送出される。その他の動作は図４に示す本発明の第３の実施の形態と同様である。

【０１０７】

（第７の実施の形態）

図１０は、本発明の第７の実施の形態における受信装置を示すブロック図である。本発明の第７の実施の形態は受信装置に受信した権利情報をダウンロード、ディジタルデータを別の受信装置にデータを変換して転送するとともにサーバに消費情報を転送することができる。図１０において、１１１～１１４は図１５に示す従来例の構成と同様であり、９０～９８、１０１～１０６、１１０、１１５、１２３～１２５、１３２は、図４に示す本発明の第３の実施の形態と同様であり、１４１は図５に示す本発明の第４の実施の形態と同様であり、１４４は第４の権利情報、２５０は第５の受信装置、２５１は第５の権利管理手段、２５２は第５の制御手段、２５３は変換手段、２５４は第２の暗号化ビデオビットストリーム、２５５は再多重化手段、２５６はＭＰＥＧ－２システムズ準拠の第３の多重化ビットストリーム、２５７は第６の受信装置、２５８は第３の要求情報である。

【０１０８】

図１０にて、読み出し情報９０は多重化分離手段１０４で分離されて第５の制御手段２５２に加えられる。第５の権利管理手段２５１は、権利情報９８を第５の受信装置２５０で使用する第１の権利情報と第６の受信装置２５７で使用する

第４の権利情報１４４に分割し、第４の権利情報１４４を再多重化手段２５５に送る。

【０１０９】

第５の制御手段２５２は第６の受信装置２５７から表２０に示す第３の要求情報２５８を受け取るものとする。表２０は第６の受信装置２５７が第５の受信装置２５０に対してツールとコンテントを要求していることを示している。第５の制御手段２５２は第５の権利管理手段２５１に権利許諾の情報を出すとともに再多重化手段２５５に再多重化の指示を含む第１の制御情報１４１を送る。

【０１１０】

【表２０】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【０１１１】

ここで、第５の受信装置２５０で１回再生し、第６の受信装置２５７で１回再生するものとすると、第１の権利情報及び第４の権利情報１４４は各々表２１、表２２となる。表２２では第５の受信装置２５０で１回再生しているので再生回数を１回減じている。

【０１１２】

【表２１】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【０１１３】

【表２２】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【０１１４】

変換手段２５３はディジタルビデオデータ１１１をＭＰＥＧ－４ビデオ（ＩＳ

Ｏ／ＩＥＣ１４４９６）に圧縮変換し更に暗号化して第２の暗号化ビデオビットストリーム２５４を出力する。

【０１１５】

復号ツール１１５は再多重化手段２５５に送られる。再多重化手段２５５は第２の暗号化ビデオビットストリーム２５４とオーディオビットストリーム１２６と第１の制御情報１４１と第４の権利情報１４４と復号ツール１１５とをＭＰＥＧ－２システムズに準拠して再多重し、再多重化信号２５６を出力する。本発明の第７の実施の形態ではディジタルオーディオビットストリーム１０６を用いているがディジタルオーディオ信号１１４を再度圧縮して用いてもよい。

【０１１６】

その他の動作は図４に示す本発明の第３の実施の形態と同様である。これによって、第５の受信装置２５０は、受信した権利情報、ビットストリーム、ツール情報等を第６の受信装置２５７に送ることが可能となる。

【０１１７】

（第８の実施の形態）

図１１は、本発明の第８の実施の形態における受信装置を示すブロック図である。図１１において、１１１～１１４は図１５に示す従来例の構成と同様であり、９０～９６、９８、１０１～１０６、１１０、１１５、１２０、１２１、１２３～１２５、１３２は、図４に示す本発明の第３の実施の形態と同様であり、３００は受信権利情報、３０１は権利情報受信手段、３０２は第７の受信装置である。また、第７の受信装置は本発明の第２の実施の形態の図３に示す送信装置８６に接続されているものとする。本発明の第８の実施の形態は本発明の第３の実施の形態と類似であるが、権利情報９８をプログラム仕様情報９２でなく受信権利情報３００から取得する点が異なる。

【０１１８】

図１１にて、入力されるＭＰＥＧ－２システムズ準拠の第１の多重化ビットストリーム１０１はハードディスク１０２に一時的に記憶された後に読み出され読み出し多重化ビットストリーム１０３として多重化分離手段１０４に加えられる。多重化分離手段１０４は読み出し多重化ビットストリーム１０３を第１の暗号

化ビデオビットストリーム１０５とオーディオビットストリーム１０６とプログラム仕様情報９２とストリーム情報９０とに分離する。

【０１１９】

ここで、プログラム仕様情報９２は、第１の暗号化ビデオビットストリーム１０５、オーディオビットストリーム６４とプログラムのプログラム番号との関係を示す情報とともに、上記プログラムに付随する権利情報９８とＡＥＳ復号を実行するツールＩＤ（０Ｘ００Ａ）を有するツールリスト９６と上記復号ツールの組み込み位置が受信装置１００の多重化分離手段１０４とビデオ復号手段１１２との間であることを示す制御グラフ９４を含むものとする。また、読み出し情報９０には、第１の暗号化ビデオビットストリーム１０５の暗号を解く為の鍵情報などが入っているものとする。

【０１２０】

読み出し情報９０は多重化分離手段１０４で分離されて第１の制御手段１２０に加えられる。プログラム仕様情報９２はプログラム仕様情報分離手段９１に加えられる。制御グラフ分離手段９３はプログラム仕様情報分離手段９１から制御グラフ９４を抽出して第１の制御手段１２０に供給する。ツールリスト分離手段９５はプログラム仕様情報分離手段９１からツールリスト９６を抽出して第１の制御手段１２０に供給する。権利情報受信手段３０１は受信権利情報３００を受信して権利情報９８を抽出して出力し第１の権利管理手段１２１に供給する。

【０１２１】

第１の制御手段１２０は表２３に示す第１の要求情報１３７を送信する。ここではツール要求とコンテンツすなわちプログラム要求を送っている。

【０１２２】

【表２３】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【０１２３】

第１の制御手段１２０は、ツールリスト９６から復号に必要なツールが復号ツール１１５であることを求め、制御グラフ９４から復号ツール１１５を適用する

制御ポイントすなわち組み込み位置が１０８であることを求めるとともに読み出し情報９０から暗号を解くための鍵情報を抽出する。

【０１２４】

第１の制御手段１２０は、復号ツール１１５の組み込み位置が第７の受信装置３０２の多重化分離手段１０４とビデオ復号手段１１２との間であることを示す制御グラフ９４に従って、組み込み手段１０８に復号ツール１１５とストリーム情報１１８から抽出された上記鍵情報を組み込む指示を出し、組み込み手段１０８は復号ツール１１５と上記鍵情報を組み込む。第１の暗号化ビデオビットストリーム１０５は組み込み手段１０８によって暗号を解読されてビットストリーム１１０として出力される。

【０１２５】

ビデオビットストリーム１１０はビデオ復号手段１１２によって伸長されディジタルビデオ信号１１１として出力される。オーディオビットストリーム１０６はオーディオ復号手段１１３によって伸長されディジタルオーディオ信号１１４として出力される。

【０１２６】

第１の権利管理手段１２１は権利情報９８を取得し、ファイル管理情報１２３をファイル管理手段１２４に出力する。ファイル管理手段１２４は、プログラムＡの場合、表４に与えられた再生回数は１回であるため、１回再生するとファイル管理手段１２４は、指令１２５をハードディスク１０２に出してハードディスク１０２上に記憶されたプログラムＡを消去する。

【０１２７】

また、第１の権利管理手段１２１は第１の返信情報１３２として表２４に示す情報を返信する。

【０１２８】

【表２４】

第７の受信装置での再生回数	0X00000001

【０１２９】

（第９の実施の形態）

図１２は、本発明の第９の実施の形態における受信装置を示すブロック図である。本発明の第９の実施の形態はネットワークに接続されている受信装置に受信した権利情報をダウンロード、ディジタルデータを転送するとともにサーバに消費情報を転送することができる。図１２において、１１１～１１４は図１５に示す従来例の構成と同様であり、９０～９６、９８、１０１～１０６、１１０、１１５、１２３～１２５、１３２は本発明の第３の実施の形態と同様であり、１３３、１３６、１３８～１４０、１４１～１４３は図５に示す本発明の第４の実施の形態と同様であり、３００、３０１は図１１に示す本発明の第８の実施の形態と同様であり、３１０は第８の受信装置、１４５は第１１の受信装置である。尚、第８の受信装置３１０は図３に示す本発明の第２の送信装置に接続されているものとし、第１１の受信装置は、図４に示す第１の受信装置と同等の機能を有するものとする。

【０１３０】

図１２にて、制御グラフ分離手段９３はプログラム仕様情報分離手段９１から制御グラフ９４を抽出して第２の制御手段１３９に供給する。ツールリスト分離手段９５はプログラム仕様情報分離手段９１からツールリスト９６を抽出して第２の制御手段１３９に供給する。権利情報受信手段３０１は受信権利情報３００を受信して権利情報９８を抽出して出力し第２の権利管理手段１３８に供給する。

【０１３１】

第２の制御手段１３９は第１１の受信装置１４５から表２５に示す第２の要求情報１４０を受け取るものとする。表２５は第１１の受信装置１４５が第２の受信装置１３０に対してツールとコンテントを要求していることを示している。

【０１３２】

【表２５】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【０１３３】

また、読み出し情報９０は多重化分離手段１０４で分離されて第２の制御手段１３９に加えられる。第２の権利管理手段１３８は、権利情報９８を第２の受信装置１３０で使用する第１の権利情報と第１１の受信装置１４５で使用する第２の権利情報１３３に分割するとともに、第１の権利情報に基づいてファイル管理情報１２３をファイル管理手段１２４に出力する。第２の権利管理手段１３８に権利許諾の指示を出すとともに多重化修正手段１４２に第１の多重化ビットストリーム１０３の修正を含む第１の制御情報１４１を送る。

【０１３４】

第８の受信装置３１０で表４に示す権利情報を有するプログラムＢを１回再生するとともに第１１の受信装置１４５に転送するものとすると、第１の権利情報を表２６、第２の権利情報１３３を表２７のように表わすことができる。第１１の受信装置１４５に転送する第２の権利情報を示す表２７では第２の受信装置１３０で１回再生するので再生回数を１回減じている。

【０１３５】

【表２６】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【０１３６】

【表２７】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【０１３７】

第２の権利管理手段１３８は表１４に示す第２の権利情報１３３を多重化修正手段１４２に送る。多重化修正手段１４２は第１の多重化ビットストリーム１０３に第２の権利情報１３３をもとに修正を加える。すなわち、第１の多重化ビットストリーム１０３の権利情報１２２を第２の権利情報１３３の内容に変更して第２の多重化ビットストリーム１４３を出力する。

【０１３８】

その他の動作は本発明の第４の実施の形態と同様である。これによって、第８の受信装置１３０は、受信した権利情報、ビットストリーム、ツール情報等をネットワーク上で接続された第１１の受信装置１４５に送ることが可能となる。

【０１３９】

また、第２の権利管理手段１３８は、第１１の受信装置１４５から送られる第２の返信情報をもとにして第１の返信情報１３２を出力する。この場合、第８の受信装置３１０及び第１１の受信装置１４５での再生回数は１回であるとすると、表２８のように構成される第１の返信情報を出力する。

【０１４０】

【表２８】

第２の受信装置での再生回数		0X00000001
第１０の受信装置での再生回数		0X00000001

【０１４１】

これによって送信装置は、第８の受信装置３１０及び第８の受信装置３１０に接続された第１１の受信装置１４５での消費情報を得ることができる。

【０１４２】

（第１０の実施の形態）

図１３は、本発明の第１０の実施の形態における受信装置を示すブロック図である。本発明の第１０の実施の形態は受信装置にホームネットワークを経由して接続された別の受信装置に関するものである。図１３において、１１１～１１４は図１５に示す従来例の構成と同様であり、９０～９６、９８、１０１～１０６、１１０、１１５、１２３～１２５、１３２は図４に示す本発明の第３の実施の形態と同様であり、１３６、１４０は図５に示す本発明の第４の実施の形態と同様であり、１５３、１５４、１６０、１６１は図８に示す本発明の第５の実施の形態と同様であり、３００、３０１は図１１に示す本発明の第８の実施の形態と同様であり、３２０は第９の受信装置である。

【０１４３】

図１３にて、制御グラフ分離手段９３はプログラム仕様情報分離手段９１から

制御グラフ９４を抽出して第３の制御手段１６０に供給する。ツールリスト分離手段９５はプログラム仕様情報分離手段９１からツールリスト９６を抽出して第３の制御手段１６０に供給する。権利情報受信手段３０１は受信権利情報３００を受信して権利情報９８を抽出して出力し第３の権利管理手段１６１に供給する。

【０１４４】

また、読み出し情報９０は第３の制御手段１６０に加えられる。第３の権利情管理手段１６１は、権利情報９８を第９の受信装置３２０で使用する第１の権利情報と第４の受信装置１５４で使用する第３の権利情報１５３とに分割し、第３の権利情報１５３を第４の受信装置１５４に送る。

【０１４５】

第３の制御手段１６０は第４の受信装置１５４から表２８に示す第２の要求情報１４０を受け取るものとする。表２９は第４の受信装置１５４が第９の受信装置３２０に対してツールとコンテントを要求していることを示している。第３の制御手段１６０は第３の権利管理手段１６１に権利許諾の情報を出す。

【０１４６】

【表２９】

ツール要求	0X10000000
コンテンツ要求	0X01000000

【０１４７】

ここでは第９の受信装置３２０で１回再生し、第４の受信装置１５４で１回再生するものとすると、第１の権利情報及び第３の権利情報１５３は各々表３０、表３１となる。表３１では第９の受信装置３２０で１回再生しているので再生回数を１回減じている。

【０１４８】

【表３０】

コピー	禁止	0X00000000
再生回数		1X00000001
編集	禁止	0X00000011

【０１４９】

【表３１】

コピー	禁止	0X00000001
再生回数		1X00000002
編集	禁止	0X00000011

【０１５０】

その他の動作は本発明の第５の実施の形態と同様である。これによって、第９の受信装置３２０は、受信した権利情報、ビットストリーム、ツール情報等を第４の受信装置１５４に送ることが可能となる。

【０１５１】

（第１１の実施の形態）

図１４は、本発明の第１１の実施の形態における受信装置を示すブロック図である。本発明の第１１の実施の形態は第１の送信装置７３と第２の受信装置１３０と第２の受信装置にネットワークによって接続された第１０の受信装置１４４に関するものである。図１４において、４９、５０は図１５に示す従来例の構成と同様であり、６６、７３、７４は図１に示す本発明の第１の実施の形態と同様であり、１１１、１１４、１３０、１３６、１４０、１４３、１４４は図５に示す本発明の第４の実施の形態と同様である。

【０１５２】

図１４にて、第１０の受信装置１４４は第２の要求情報１４０を第２の受信装置１３０に出力する。第２の受信装置１３０は状態情報７４を第１の送信装置７３に出力する。第１の送信装置７３は、本発明の第１の実施の形態と同様に第１の多重化ビットストリーム６６を出力する。第２の受信装置１３０が受信する第１の多重化ビットストリーム６６は本発明の第４の実施の形態では１０１と記されており、本発明の第４の実施の形態と同様に処理されてビデオ復号手段１１１とディジタルオーディオ信号１１４を出力すると共に第２の多重化ビットストリーム１４３として第１０の受信装置１４４に出力される。第１０の受信装置１４４は、本発明の第３の実施の形態と同様に動作し、第２の返信情報１３６を出力する。

【０１５３】

【発明の効果】

以上説明したところから明らかなように、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部として受信装置にダウンロードすることができるのでツールを更新することが可能であり、常に最新の保護方式を提供することのできる信頼性の高い送信装置を提供することができる。

【０１５４】

また、本発明は、上記効果に加えて、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報のプログラム仕様情報の一部として処理することができるという利便性を提供することができる。

【０１５５】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るので、権利情報を多重化情報とは別に扱うことができるので受信装置で権利情報を書き換えて別の受信装置に転送する場合に再多重化を行う必要がないという利便性を有する送信装置を提供することができる。

【０１５６】

また、本発明は、上記効果に加えて、権利情報を上記多重化情報とは別のファイルで送るとともに権利情報と多重化情報との対応付けも行うことができるので、複数の多重化情報と権利情報が混在する場合にも各々区別することができるという利便性を有する送信装置を提供することができる。

【０１５７】

また、本発明は、上記効果に加えて、暗号を復号する復号ツールも同時に多重化して送信する利便性を有する送信装置を提供することができる。

【０１５８】

また、本発明は、上記効果に加えて、暗号を復号するための鍵情報も同時に多重化して送信する利便性を有する送信装置を提供することができる。

【０１５９】

本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報を多重化情報の一部としてダウンロードすることができるので更新可能であり、常に最新の保護方式を組み込むことができる信頼性の高い受信装置を提供することができる。

【０１６０】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報と権利情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持することが可能であるばかりでなく、多重化情報のプログラム仕様情報の一部として処理できる利便性を有する受信装置を提供することができる。

【０１６１】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持することができるばかりでなく、権利情報を上記多重化情報とは別のファイルで受信することができるので権利情報を多重化情報とは別に扱うことができるという利便性と別の受信装置に転送する場合の任意性を与えることができる受信装置を提供することができる。

【０１６２】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、権利情報に基づいて受信した暗号化データを消去することができるので使用済みのコンテンツを受信装置に残すことがなく不正な使用を防止することができる信頼性の高い受信装置を提供することができる。

【０１６３】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信した暗号化データの消費情報を送信装置に送り受信装置の消費状況を提供する受信装

置を提供することができる。

【０１６４】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報を別の受信装置にダウンロードすることができるので更新可能であり、常に最新の保護方式を維持できることに加えて、別の受信装置が受信した暗号化データの消費情報を送信装置に送り受信装置の消費状況を提供する受信装置を提供することができる。

【０１６５】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信した権利情報を分割して別の受信装置に暗号化データとともに送信することができるので別の受信装置でも同様に暗号化データを高信頼性のもとに処理することのできる受信装置を提供することができる。

【０１６６】

また、本発明は、暗号化されたデータとともに暗号を復号するためのツールリスト、ツール、ツール組み込み位置、鍵情報をダウンロードすることができるので、更新可能であり、常に最新の保護方式を維持できることに加えて、受信装置が受信したデータを変換することにより別の受信装置に最適な信号として転送することが可能な受信装置を提供することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態における送信装置の概略構成を示す図

【図２】

本発明の第１の実施の形態における制御グラフ

【図３】

本発明の第２の実施の形態における送信装置の概略構成を示す図

【図４】

本発明の第３の実施の形態における受信装置の概略構成を示す図

【図５】

本発明の第４の実施の形態における受信装置の概略構成を示す図

【図６】

本発明の第４の実施の形態における第２の権利管理手段の概略処理を示す図

【図７】

本発明の第４の実施の形態における多重化ビットストリームの概略構成を示す図

【図８】

本発明の第５の実施の形態における受信装置の概略構成を示す図

【図９】

本発明の第６の実施の形態における受信装置の概略構成を示す図

【図１０】

本発明の第７の実施の形態における受信装置の概略構成を示す図

【図１１】

本発明の第８の実施の形態における受信装置の概略構成を示す図

【図１２】

本発明の第９の実施の形態における受信装置の概略構成を示す図

【図１３】

本発明の第１０の実施の形態における受信装置の概略構成を示す図

【図１４】

本発明の第１１の実施の形態におけるシステム構成を示す図

【図１５】

従来の構成図

【符号の説明】

５１　権利情報生成手段

５３　制御グラフ生成手段

５４　制御情報生成手段

６０　暗号化手段

６３　暗号化ビデオビットストリーム

７３　第１の送信装置

７４　状態情報

８５　送信権利情報

９０　読み出し情報

９５　ツールリスト分離手段

９７　権利情報分離手段

１０１　第１の多重化ビットストリーム

１０８　組み込み手段

１１５　復号ツール

１２０　第１の制御手段

１２１　第１の権利管理手段

１２４　ファイル管理手段

１３２　第１の返信情報

１３３　第２の権利情報

１３６　第２の返信情報

１３７　第１の要求情報

１３８　第２の権利管理手段

１３９　第２の制御手段

１４０　第２の要求情報

１４１　第１の制御情報

１４３　第２の多重化ビットストリーム

１５３　第３の権利情報

１６０　第３の制御手段

１６１　第３の権利管理手段

２３１　第４の制御手段

２３２　第４の権利管理手段

２５１　第５の権利管理手段

２５２　第５の制御手段

２５４　第２の暗号化ビデオビットストリーム

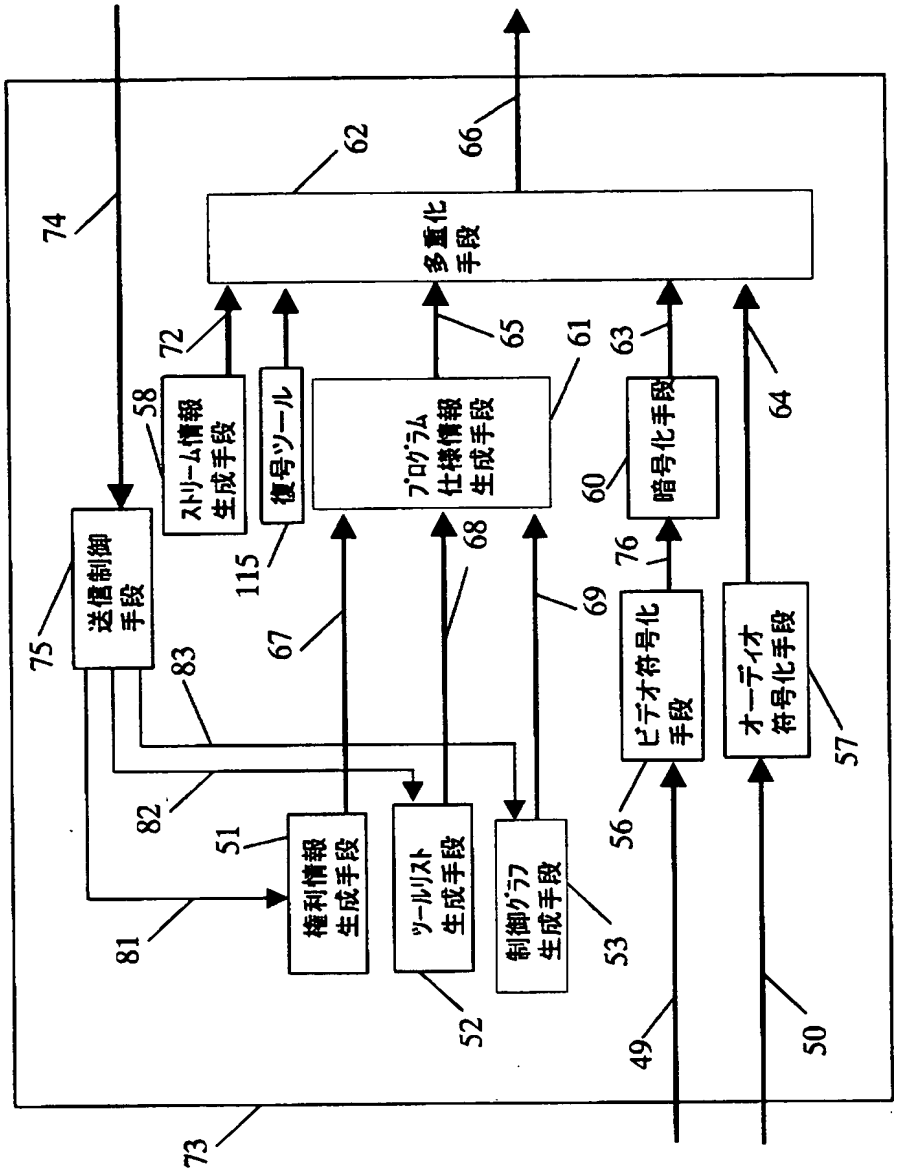
２５５　再多重化手段

２５６　第３の多重化ビットストリーム

２５８　第３の要求情報

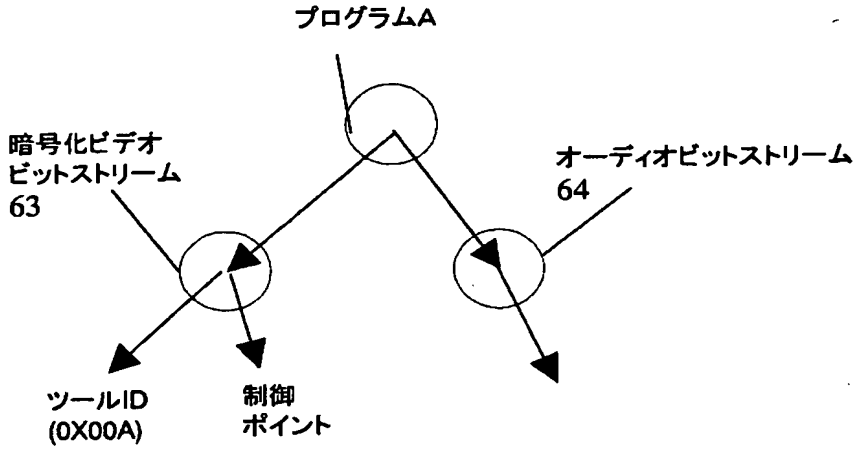
【書類名】　　図面

【図１】



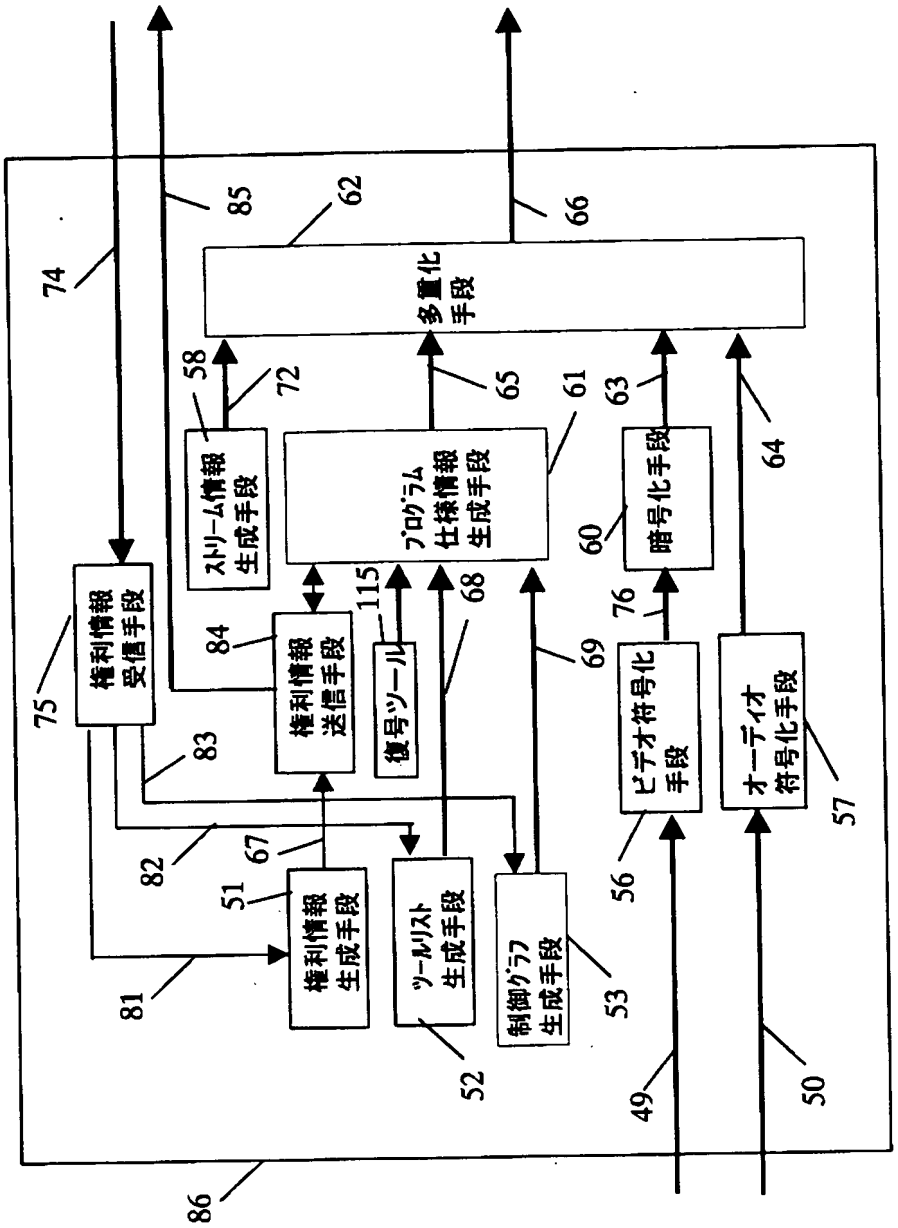
出証特２００３－３０４６８９５

【図２】

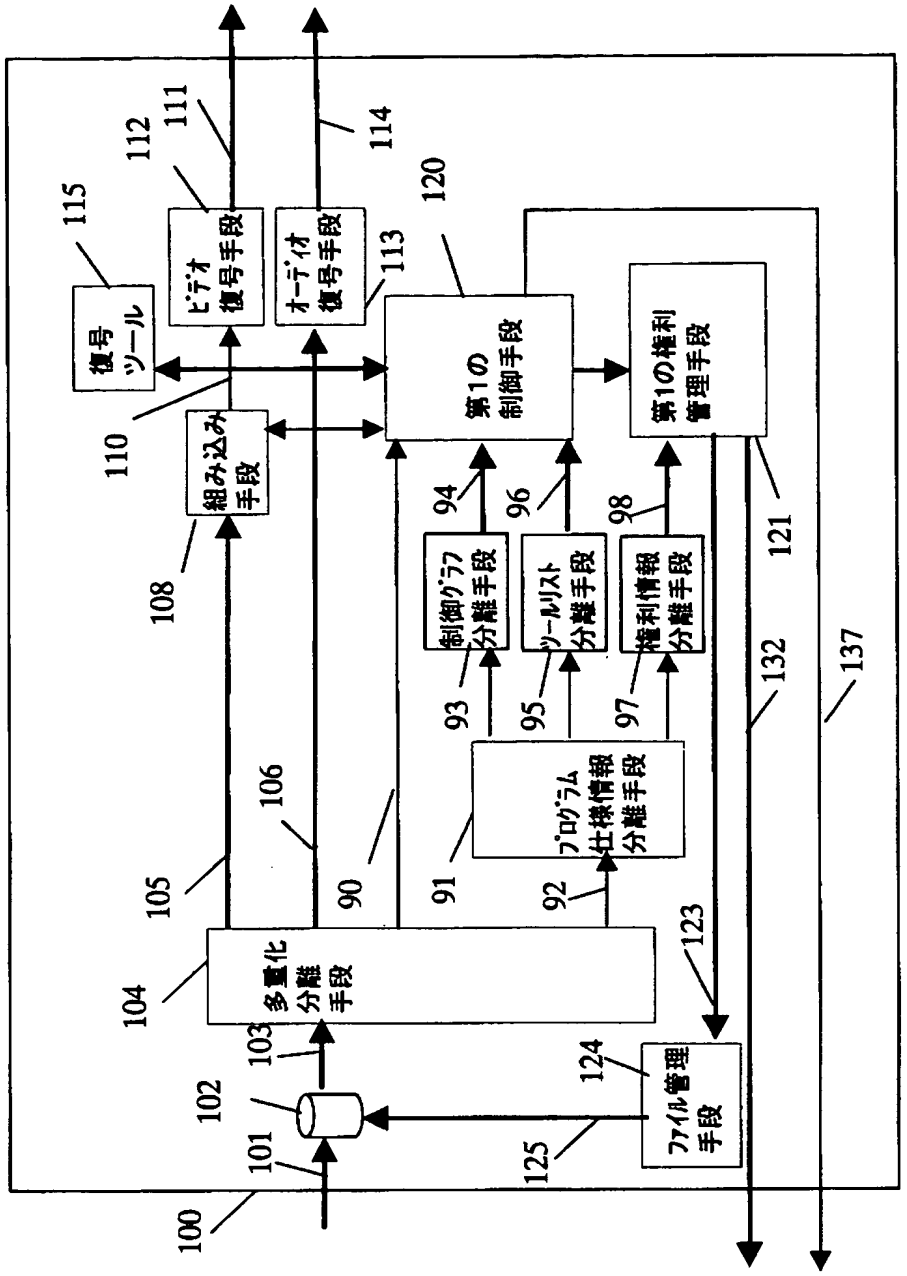


出証特２００３－３０４６８９５

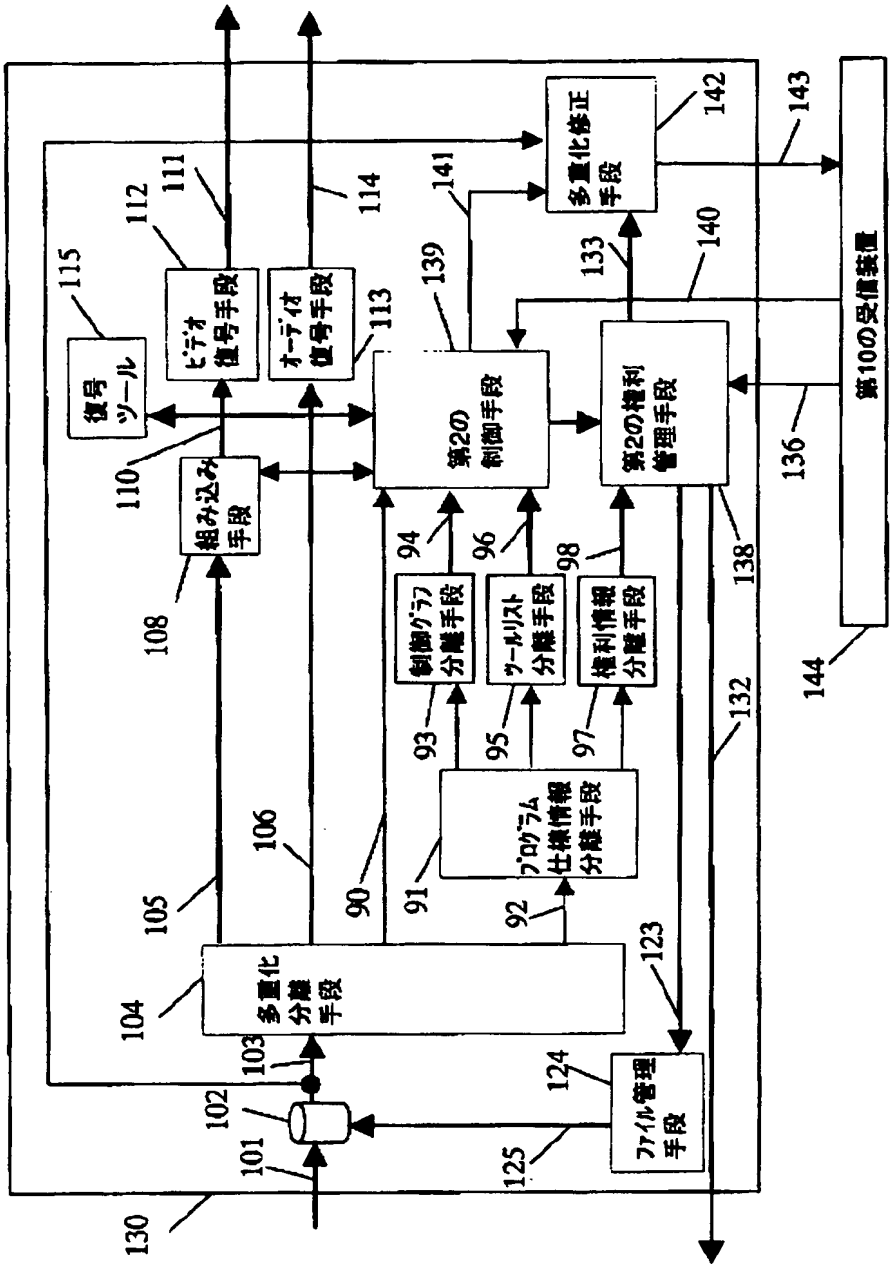
【図３】


多重化手段
ストリーム情報生成手段
プログラム仕様情報生成手段
暗号化手段
権利情報受信手段
権利情報送信手段
復号ツール
ビデオ符号化手段
オーディオ符号化手段
権利情報生成手段
ツールリスト生成手段
制御グラフ生成手段
74
85
62
66
58
72
65
61
63
64
60
75
84
115
68
76
69
83
82
67
51
56
57
81
53
52
49
50
86

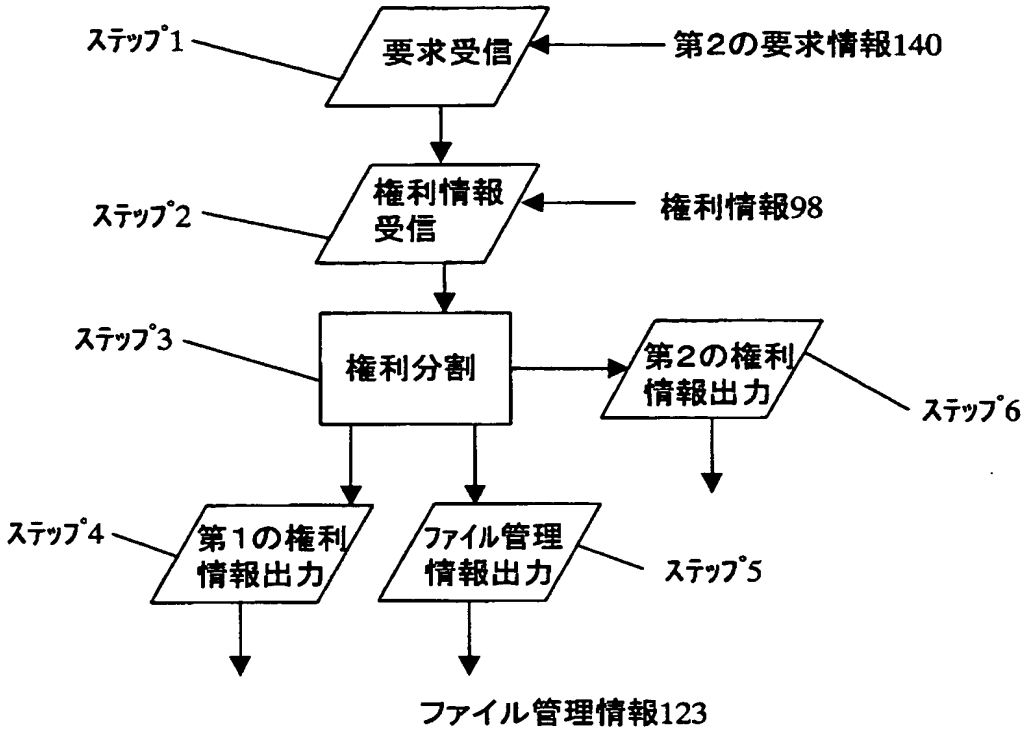
【図４】


復号ツール
ビデオ復号手段
オーディオ復号手段
第1の制御手段
第1の権利管理手段
組み込み手段
制御ログ分離手段
ツールリスト分離手段
権利情報分離手段
プログラム仕様情報分離手段
多重化分離手段
ファイル管理手段
100
101
102
103
104
105
106
108
110
111
112
113
114
115
120
121
123
124
125
132
137
90
91
92
93
94
95
96
97
98

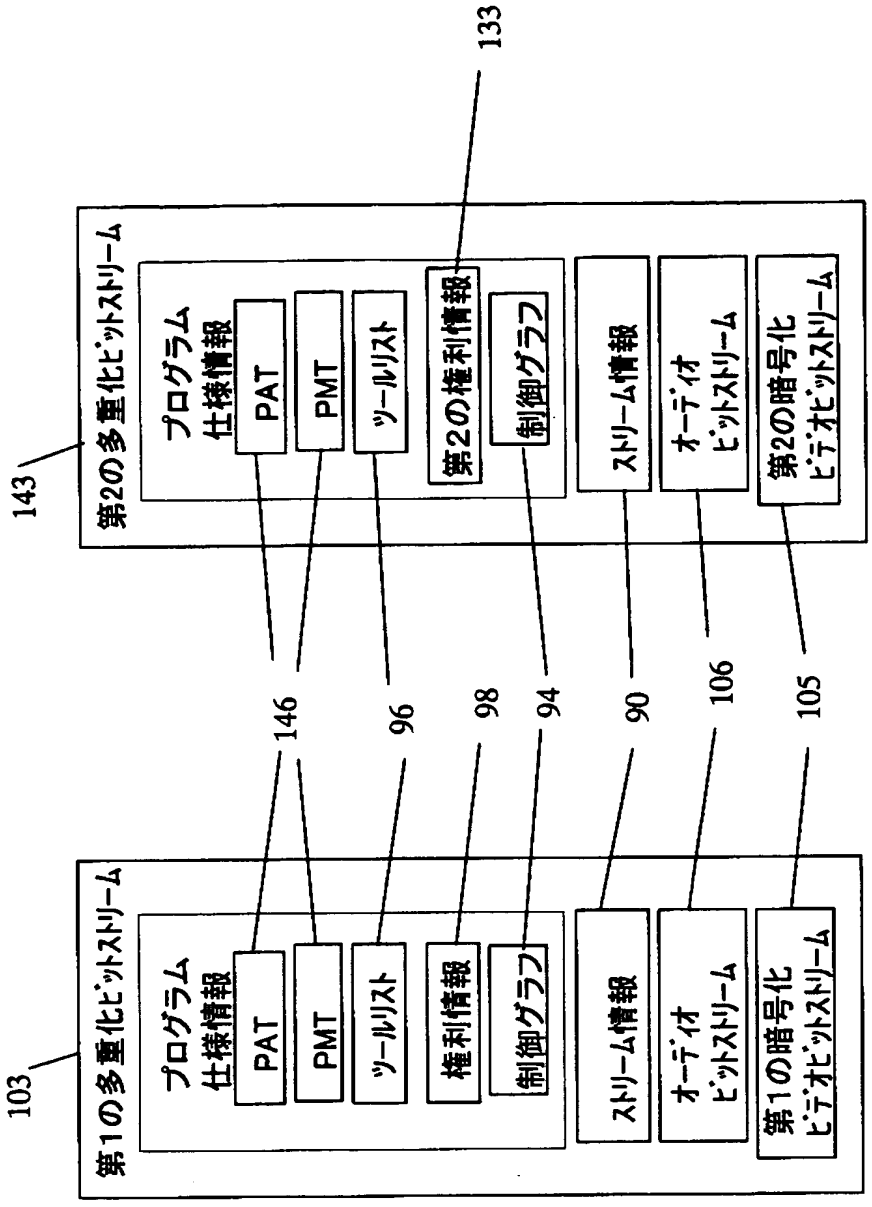
【図５】


多重化分離手段
多重化修正手段
ビデオ復号手段
オーディオ復号手段
復号ツール
組み込み手段
第20の制御手段
第20の権利管理手段
制御グラフ分離手段
ツールリスト分離手段
権利情報分離手段
プログラム仕様情報分離手段
ファイル管理手段
第100の受信装置
101
102
103
104
105
106
108
110
111
112
113
114
115
123
124
125
130
132
133
136
138
139
140
141
142
143
144

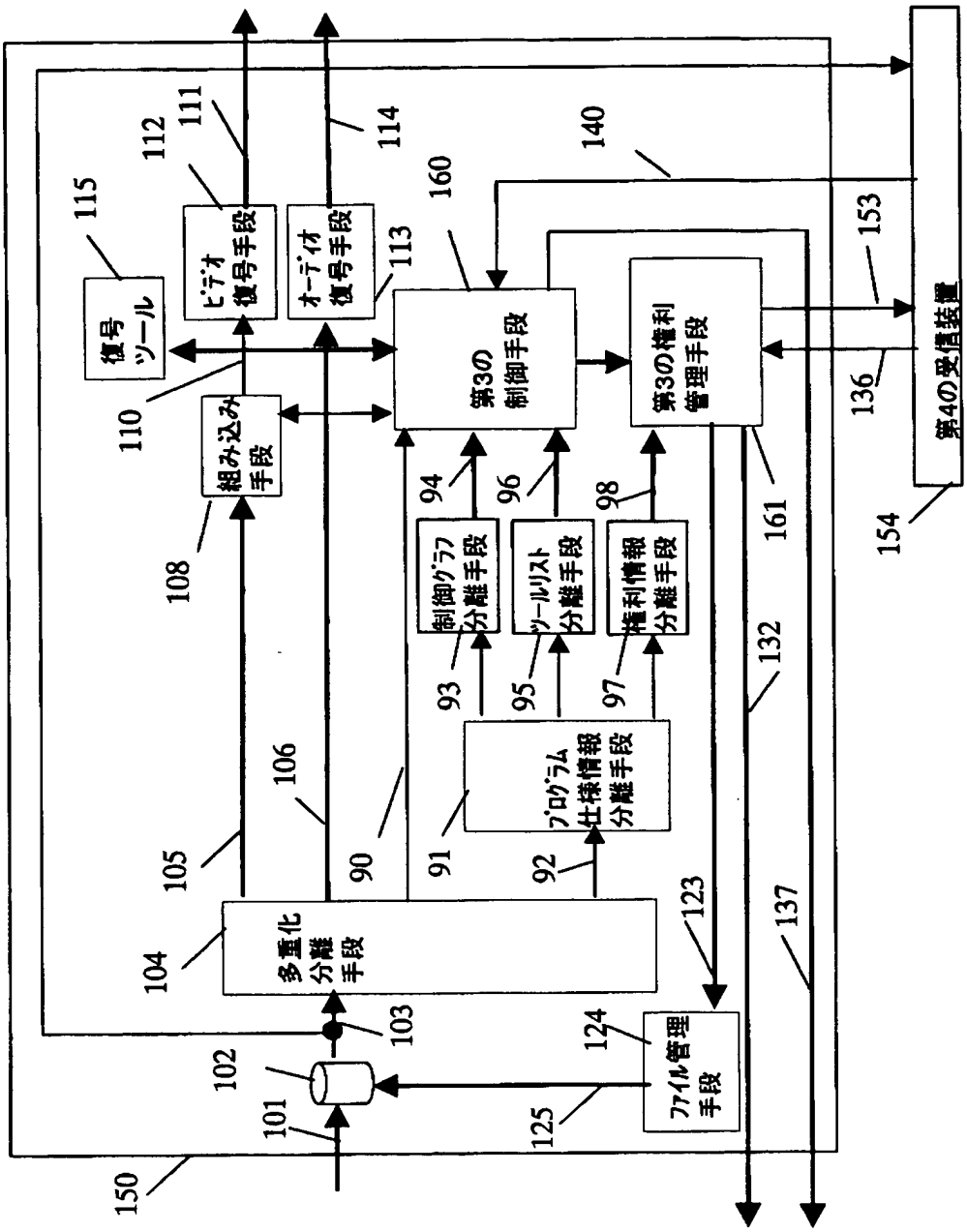
【図６】


ステップ1
要求受信
第2の要求情報140
ステップ2
権利情報受信
権利情報98
ステップ3
権利分割
第2の権利情報出力
ステップ6
ステップ4
第1の権利情報出力
ファイル管理情報出力
ステップ5
ファイル管理情報123

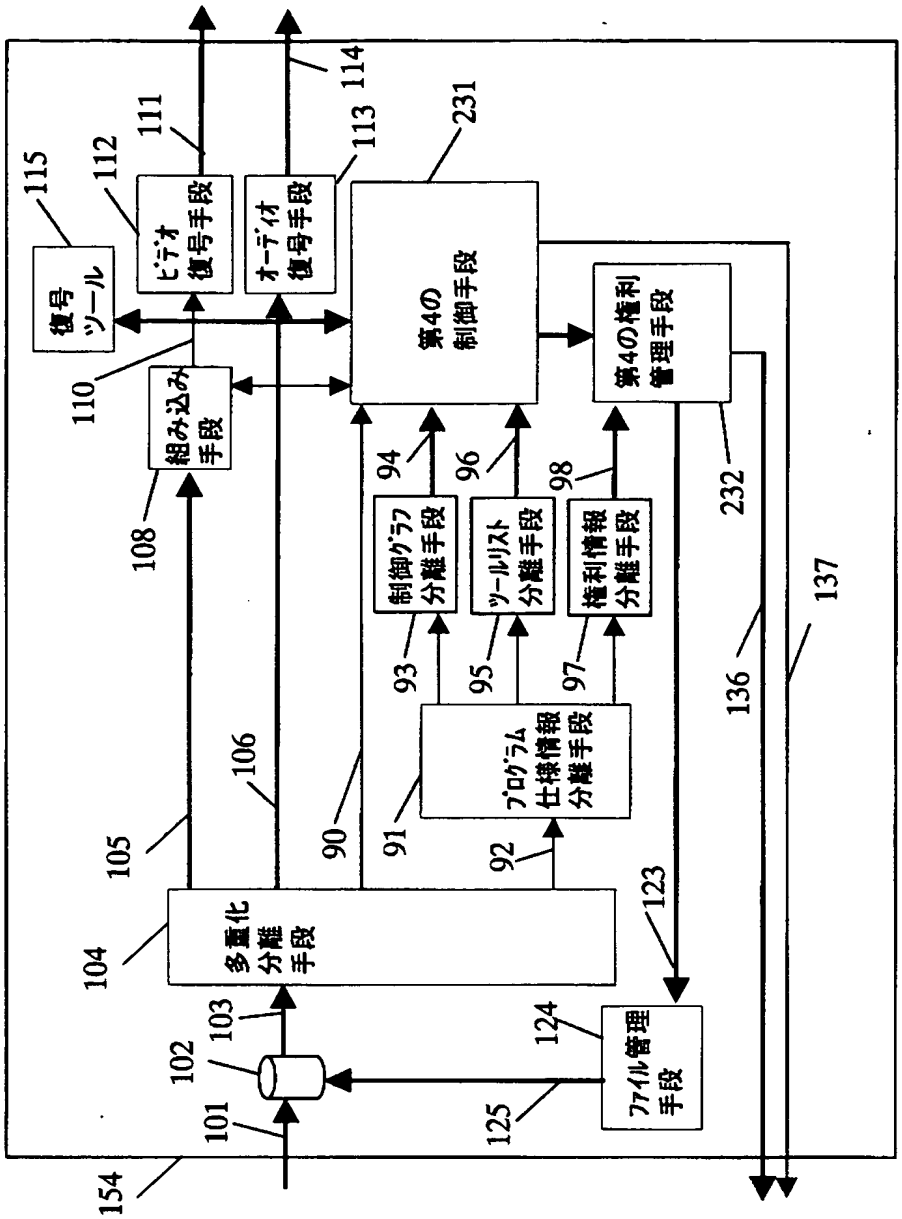
【図７】


143
第2の多重化ビットストリーム
プログラム仕様情報
PAT
PMT
ツールリスト
第2の権利情報
制御グラフ
ストリーム情報
オーディオビットストリーム
第2の暗号化ビデオビットストリーム
133
146
96
98
94
90
106
105
103
第1の多重化ビットストリーム
プログラム仕様情報
PAT
PMT
ツールリスト
権利情報
制御グラフ
ストリーム情報
オーディオビットストリーム
第1の暗号化ビデオビットストリーム

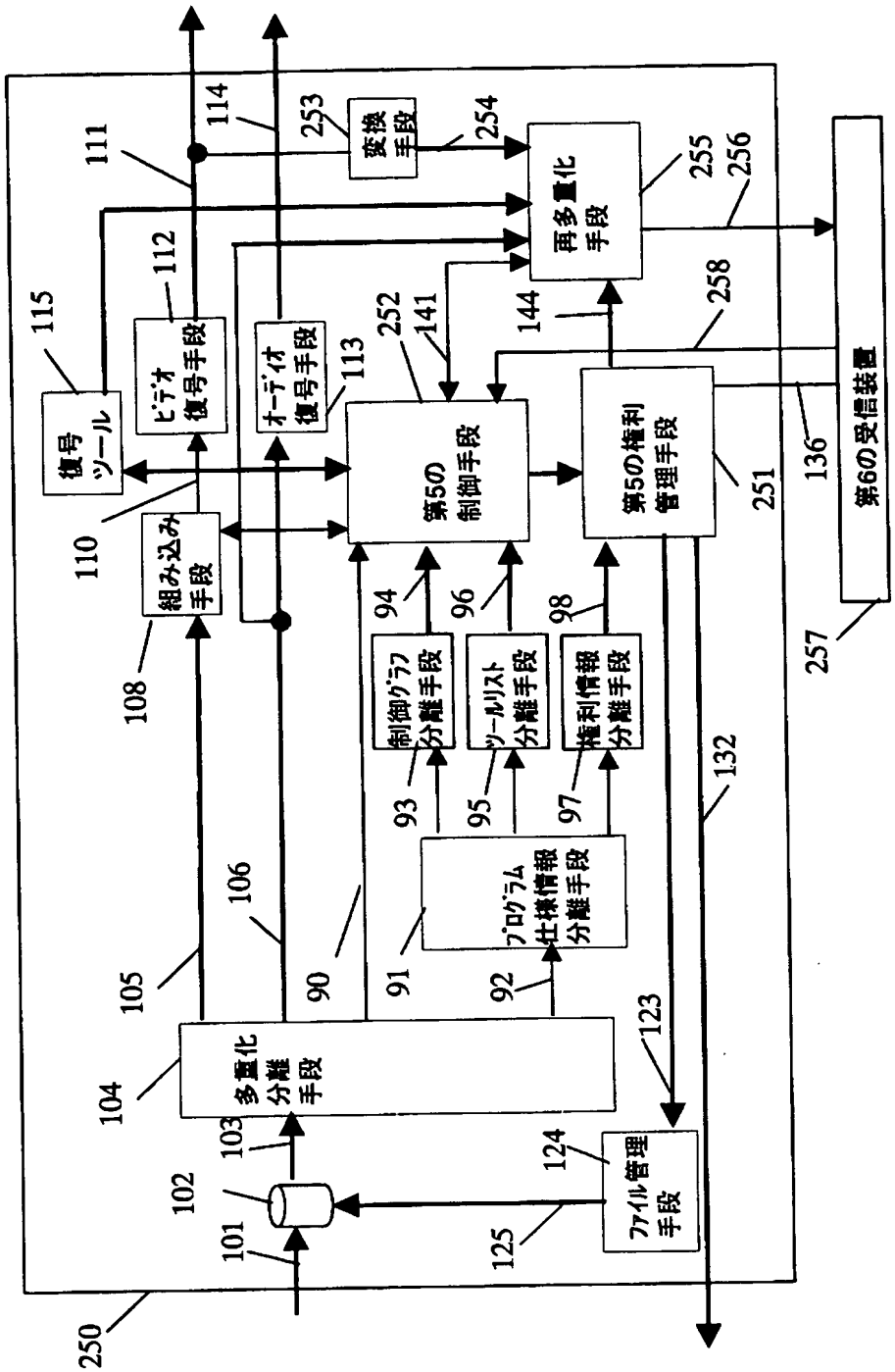
【図８】


復号ツール
ビデオ復号手段
オーディオ復号手段
組み込み手段
第3の制御手段
第3の権利管理手段
第4の受信装置
制御グラフ分離手段
ツールリスト分離手段
権利情報分離手段
プログラム仕様情報分離手段
多重化分離手段
ファイル管理手段
150
101
102
103
104
105
106
108
110
111
112
113
114
115
90
91
92
93
94
95
96
97
98
123
124
125
132
136
137
140
153
154
160
161

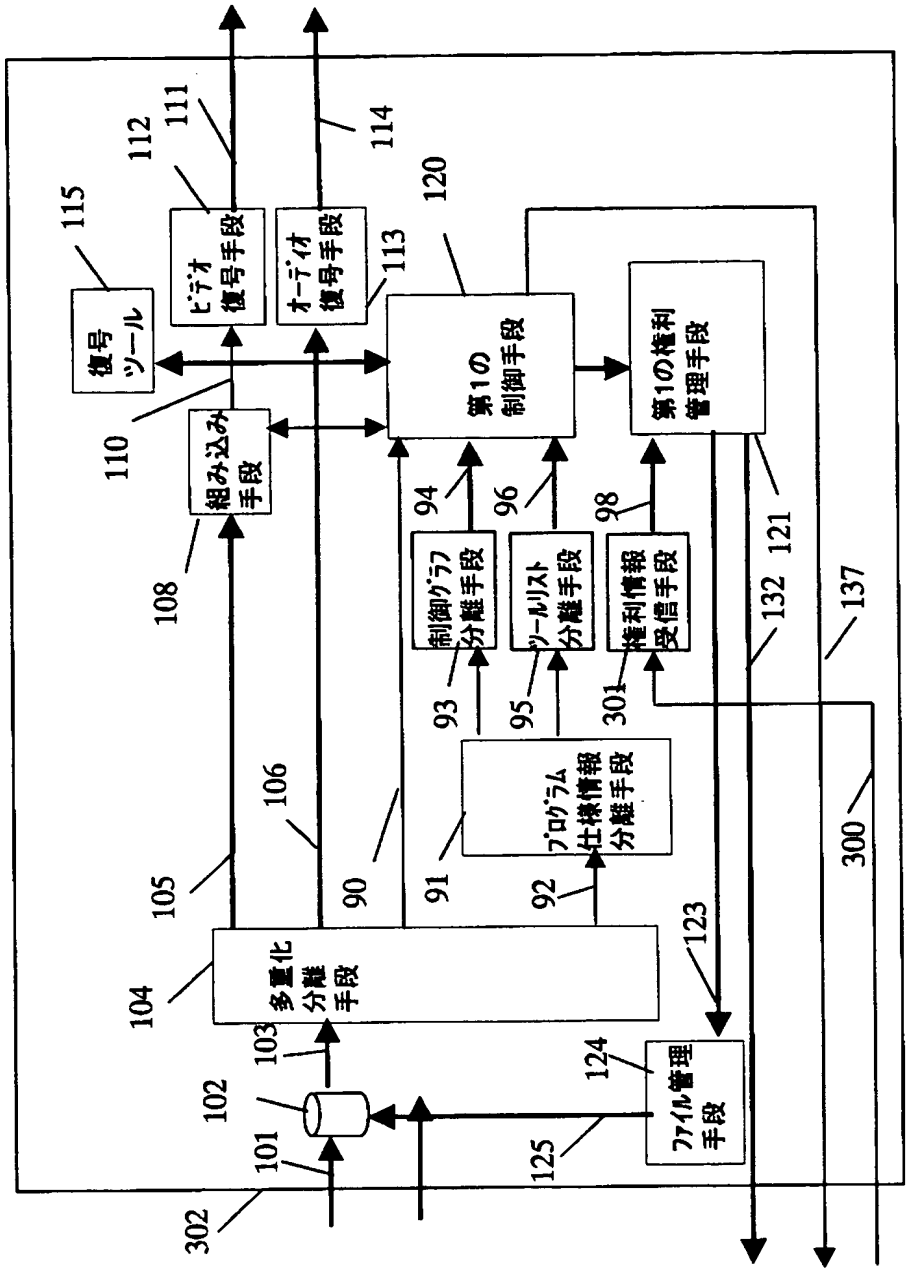
【図９】


復号ツール
ビデオ復号手段
オーディオ復号手段
第4の制御手段
第4の権利管理手段
組み込み手段
制御グラフ分離手段
ツールリスト分離手段
権利情報分離手段
プログラム仕様情報分離手段
多重化分離手段
ファイル管理手段
154
101
102
103
104
105
106
108
110
111
112
113
114
115
90
91
92
93
94
95
96
97
98
123
124
125
136
137
231
232

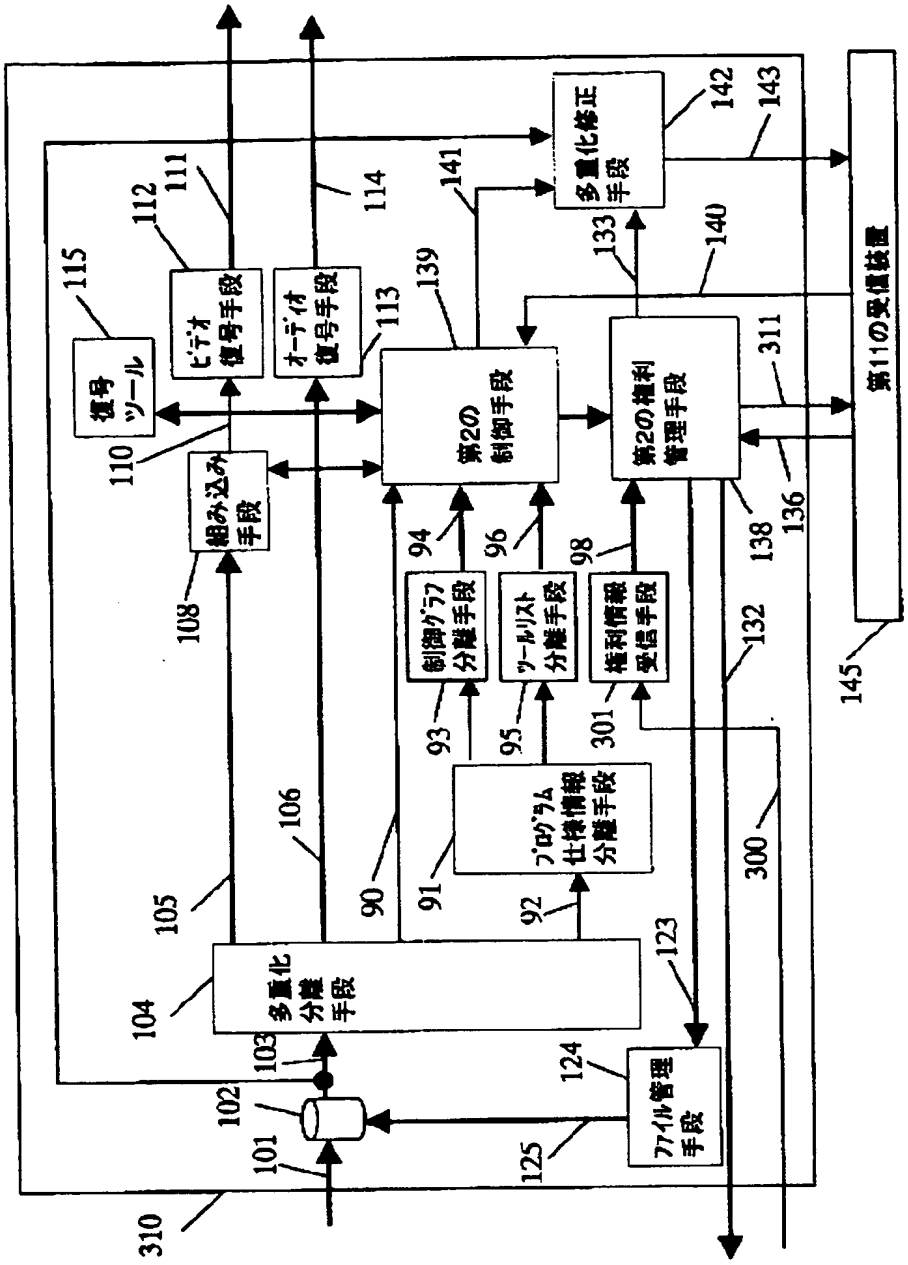
【図１０】


250
101
102
103
104
105
106
90
91
92
93
94
95
96
97
98
108
110
111
112
113
114
115
123
124
125
132
136
141
144
251
252
253
254
255
256
257
258
多重化分離手段
ファイル管理手段
プログラム仕様情報分離手段
制御グラフ分離手段
ツールリスト分離手段
権利情報分離手段
組み込み手段
復号ツール
ビデオ復号手段
オーディオ復号手段
第5の制御手段
第5の権利管理手段
変換手段
再多重化手段
第6の受信装置

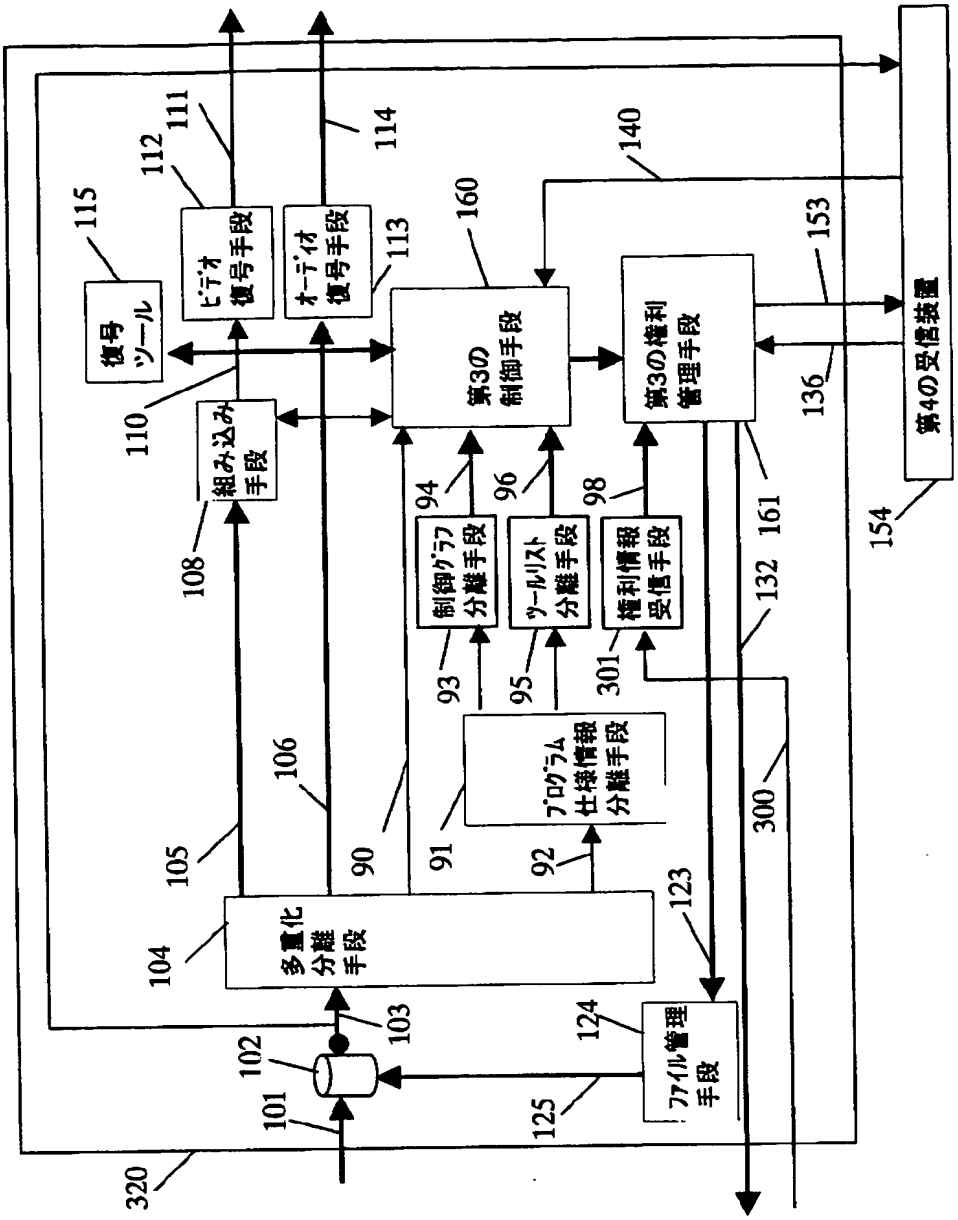
【図１１】


復号ツール
ビデオ復号手段
オーディオ復号手段
組み込み手段
第1の制御手段
第1の権利管理手段
制御グラフ分離手段
ツールリスト分離手段
権利情報受信手段
プログラム仕様情報分離手段
多重化分離手段
ファイル管理手段
111
112
114
115
120
113
110
108
94
96
98
121
132
137
93
95
301
106
105
90
91
92
300
123
104
103
124
102
101
125
302

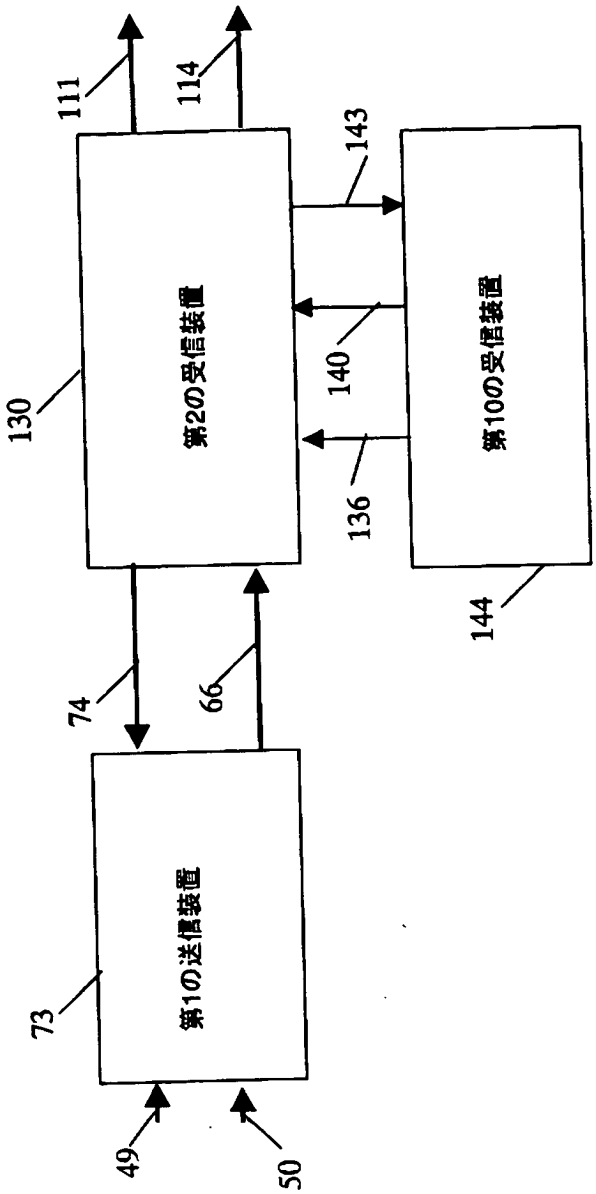
【図１２】


310
101
102
103
104
105
106
107
108
110
111
112
113
114
115
139
140
141
142
143
145
300
301
311
多重化分離手段
ファイル管理手段
組み込み手段
ビデオ復号手段
オーディオ復号手段
復号ツール
第2の制御手段
多重化修正手段
第2の権利管理手段
第11の受信装置
プログラム仕様情報分離手段
ツールリスト分離手段
権利情報受信手段

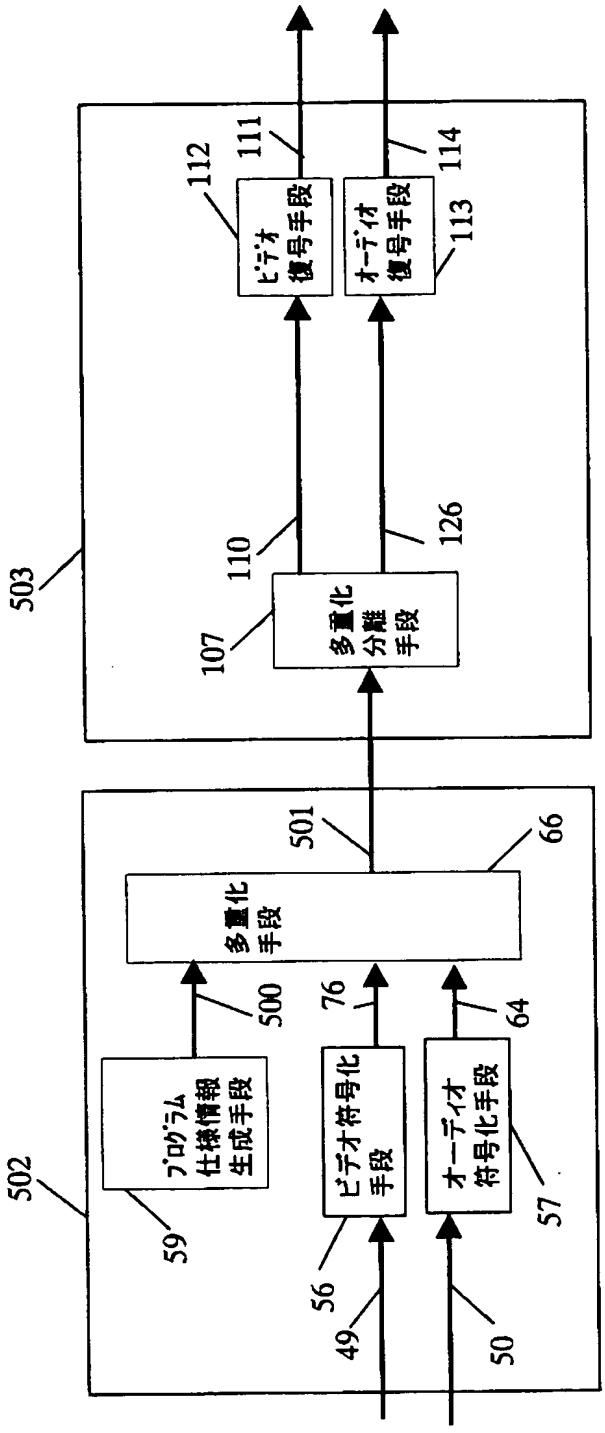
【図１３】


復号ツール
ビデオ復号手段
オーディオ復号手段
組み込み手段
第3の制御手段
第3の権利管理手段
第4の受信装置
制御グラフ分離手段
ツールリスト分離手段
権利情報受信手段
プログラム仕様情報分離手段
多重化分離手段
ファイル管理手段
111
112
114
115
140
160
153
113
110
136
154
94
96
98
108
161
132
93
95
301
106
300
105
90
91
92
123
104
103
124
102
101
125
320

【図１４】


111
114
143
第2の受信装置
第10の受信装置
130
140
136
144
74
66
第1の送信装置
73
49
50

【図１５】


503
112
111
114
113
ビデオ復号手段
オーディオ復号手段
110
126
107
多重化分離手段
501
66
多重化手段
500
76
64
502
プログラム仕様情報生成手段
ビデオ符号化手段
オーディオ符号化手段
59
56
57
49
50

【書類名】　要約書

【要約】

【課題】　暗号化の仕組みを破られた場合に、暗号化の仕組みを更新する送受信装置を提供すること。

【解決手段】　暗号化データの復号ツールのツールＩＤを取得、存在の確認とツールの取得、更新を行うとともに、上記暗号化データに付随する権利情報に基づいて上記暗号化データの処理と転送を行う。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社